Version : **2021.01**

Dernière mise-à-jour : 2021/02/05 08:45

SER703 - Les Commandes ldap* et slap*

Contenu du Module

- **SER703 - Les Commandes ldap* et slap** *
  - Contenu du Module
  - Présentation
  - LAB #1 - La Commande ldapadd
    - 1.1 - Installation et Utilisation du client graphique luma
      - Le Directory Information Tree
      - Les alias
    - 1.2 - Installation et Utilisation du Client HTML phpLDAPadmin
      - Les attributs
      - Les classes
      - Les schémas
      - Les referrals
  - LAB #2 - La Commande ldapsearch
  - LAB #3 - La Commande ldapmodify
  - LAB #4 - La Commande ldapdelete
  - LAB #5 - La Commande slapadd
  - LAB #6 - Maintenance d’une base de données LDAP
    - 6.1 - La commande slapcat
    - 6.2 - La commande slapindex
    - 6.3 - La commande slapdn
    - 6.4 - La commande slaptest
    - 6.5 - La commande slapauth

Présentation

Les commandes ldap* sont utilisées quand le serveur OpenLDAP fonctionne tandis que les commandes slap* sont utilisées pour apporter des modifications quand le serveur est arrêté.

LAB #1 - La Commande ldapadd

Afin de pouvoir utiliser notre fichier LDIF, il est nécessaire de faire appel au client **ldapadd**. Cet utilitaire prend un ou plusieurs options :

```
[root@centos7 ~]# ldapadd --help
ldapadd: invalid option -- '-'
ldapadd: unrecognized option --
Add or modify entries from an LDAP server

usage: ldapadd [options]
    The list of desired operations are read from stdin or from the file
    specified by "-f file".
Add or modify options:
  -a         add values (default)
  -c         continuous operation mode (do not stop on errors)
  -E [!]ext=extparam    modify extensions (! indicate s criticality)
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -S file    write skipped modifications to `file'
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
```

```
            [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
            [!]manageDSAit         (RFC 3296)
            [!]noop
            ppolicy
            [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
            [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
            [!]relax
            [!]sessiontracking
            abandon, cancel, ignore (SIGINT sends abandon/cancel,
            or ignores response; if critical, doesn't wait for SIGINT.
            not really controls)
-h host     LDAP server
-H URI      LDAP Uniform Resource Identifier(s)
-I          use SASL Interactive mode
-n          show what would be done but don't actually do it
-N          do not use reverse DNS to canonicalize SASL host name
-O props    SASL security properties
-o <opt>[=<optparam>] general options
            nettimeout=<timeout> (in seconds, or "none" or "max")
            ldif-wrap=<width> (in columns, or "no" for no wrapping)
-p port     port on LDAP server
-Q          use SASL Quiet mode
-R realm    SASL realm
-U authcid SASL authentication identity
-v          run in verbose mode (diagnostics to standard output)
-V          print version info (-VV only)
-w passwd   bind password (for simple authentication)
-W          prompt for bind password
-x          Simple authentication
-X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
-y file     Read password from file
-Y mech     SASL mechanism
```

```
  -Z         Start TLS request (-ZZ to require successful response)
```

Editez ensuite **setup.ldif** de la façon suivante :

```
[root@centos7 ~]# vi setup.ldif
[root@centos7 ~]# cat setup.ldif
# Organisation i2tch
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

# Gestionnaire de l'arbre
dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
```

Il convient maintenant d'utiliser la commande ldapadd afin d'injecter le contenu du fichier setup.ldif dans notre base :

```
[root@centos7 ~]# ldapadd -f setup.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "dc=i2tch,dc=com"

adding new entry "cn=Manager,dc=i2tch,dc=com"
```

Nous procédons maintenant de la même façon pour les autres données. Créez le fichier **import.ldif** :

```
[root@centos7 ~]# vi import.ldif
[root@centos7 ~]# cat import.ldif
version: 1
dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
```

```
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
```

```
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Il convient maintenant d'utiliser de nouveau la commande ldapadd afin d'injecter le contenu du fichier import.ldif dans notre base :

```
[root@centos7 ~]# ldapadd -f import.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "ou=France,dc=i2tch,dc=com"

adding new entry "ou=Commercial,ou=France,dc=i2tch,dc=com"

adding new entry "ou=Recherche,ou=France,dc=i2tch,dc=com"

adding new entry "ou=Production,ou=France,dc=i2tch,dc=com"

adding new entry "ou=Suisse,dc=i2tch,dc=com"

adding new entry "ou=Commercial,ou=Suisse,dc=i2tch,dc=com"

adding new entry "ou=USA,dc=i2tch,dc=com"

adding new entry "ou=Commercial,ou=USA,dc=i2tch,dc=com"

adding new entry "ou=Recherche,ou=USA,dc=i2tch,dc=com"
```

1.1 - Installation et Utilisation du client graphique luma

Configurez votre machine virtuelle pour démarrer en mode graphique :

```
[root@centos7 ~]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 37 Apr 30  2016 /etc/systemd/system/default.target -> /lib/systemd/system/multi-
user.target
[root@centos7 ~]# rm -rf /etc/systemd/system/default.target
[root@centos7 ~]# ln -s /lib/systemd/system/graphical.target /etc/systemd/system/default.target
[root@centos7 ~]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 36 Jan  9 18:09 /etc/systemd/system/default.target ->
/lib/systemd/system/graphical.target
```

Arrêtez votre machine virtuelle :

```
[root@centos7 ~]# exit
[trainee@centos7 ~]$ exit
desktop@serverXX:~$ VBoxManage controlvm CentOS_7 poweroff
```

Augmentez sa mémoire à 2Go :

```
desktop@serverXX:~$ VBoxManage modifyvm CentOS_7 --memory 2048
```

Démarrez ensuite la VM :

```
desktop@serverXX:~$ VBoxManage startvm CentOS_7 --type headless
Waiting for VM "CentOS_7" to power on...
VM "CentOS_7" has been successfully started
```

Connectez-vous à votre VM :

```
desktop@serverXX:~$ ssh -l trainee localhost -p 3022
```

Téléchargez ensuite **luma-master.zip** :

```
[trainee@centos7 ~]$ su -
Mot de passe : fenestros
```

```
[root@centos7 ~]# wget https://www.dropbox.com/s/wffzwfkad23ypwg/luma-master.zip
```

Installez le paquet **PyQt4** :

```
[root@centos7 ~]# yum install PyQt4
```

Décompressez l'archive **luma-master.zip** :

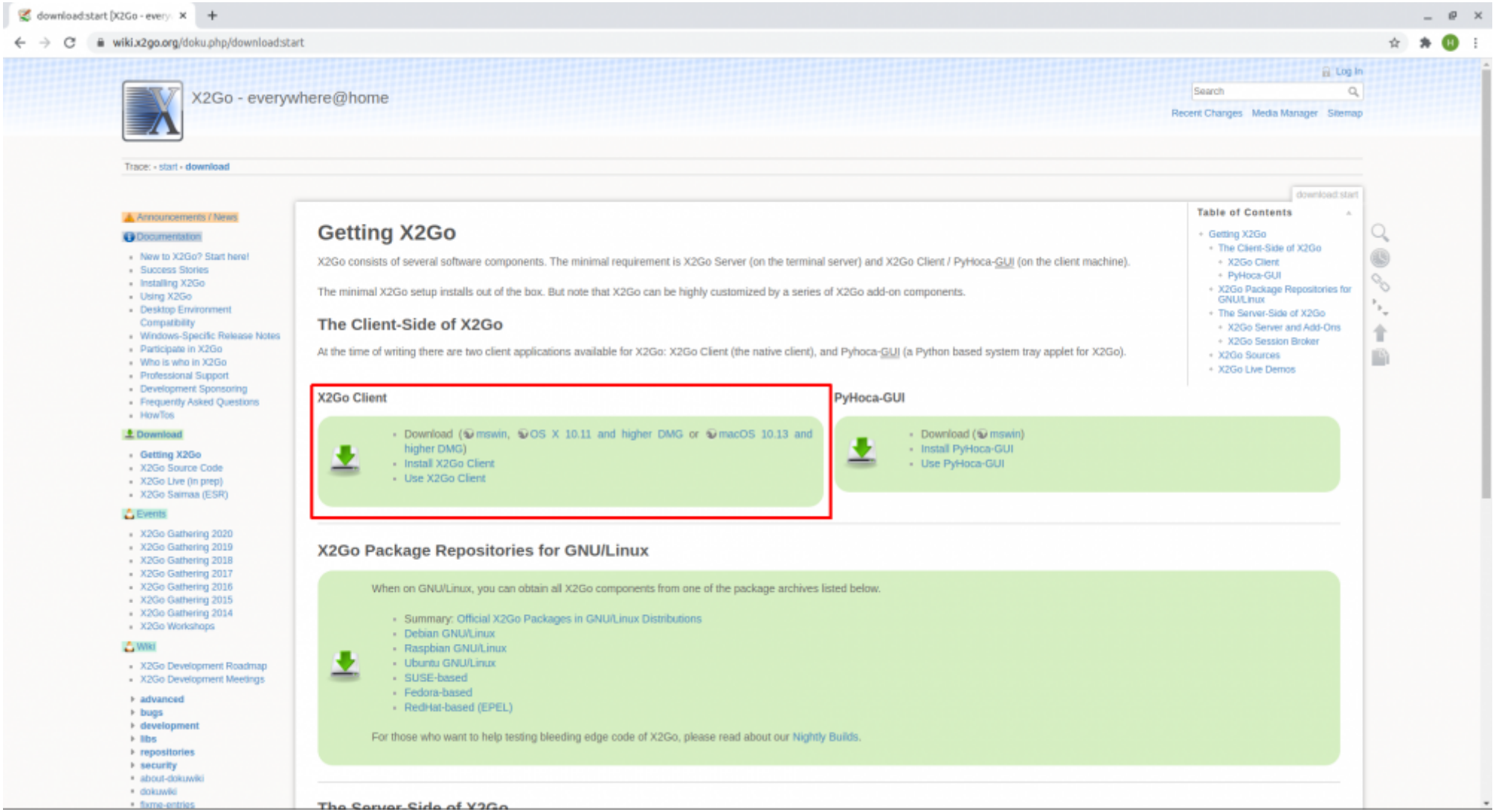
```
[root@centos7 ~]# unzip luma-master.zip
```

Installez luma :

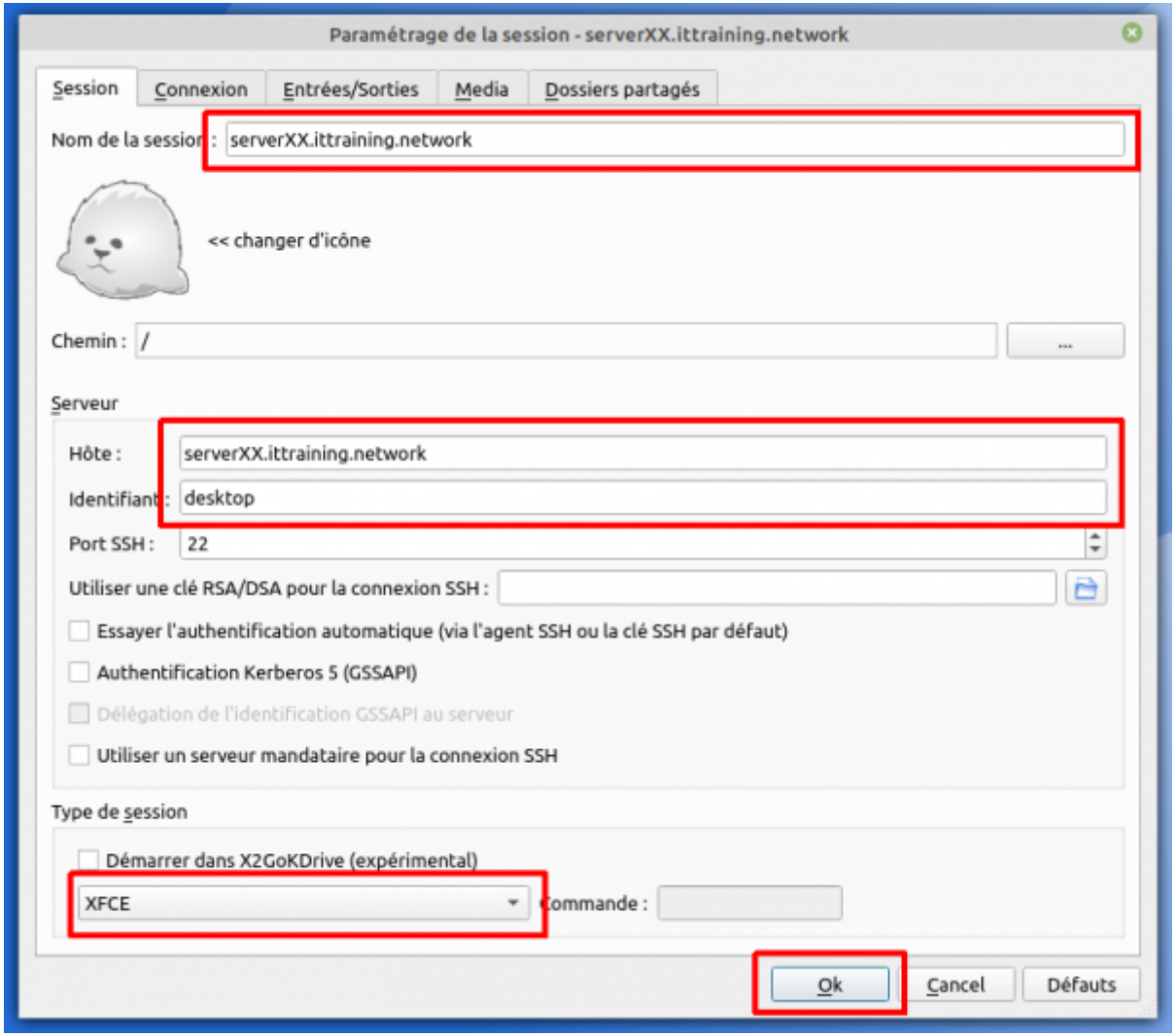
```
[root@centos7 ~]# cd luma-master/
[root@centos7 luma-master]# ls
AUTHORS  bumpversion.sh  contrib  data  HACKING  luma      luma.qrc  MANIFEST.in  resources  setup.py  tools
bin      ChangeLog       COPYING  doc   INSTALL  luma.pro  Makefile  README       setup      TODO
[root@centos7 luma-master]# python setup.py install
```

Connectez-vous à votre serveur cloud en mode graphique en utilisant l'utilitaire X2Go.

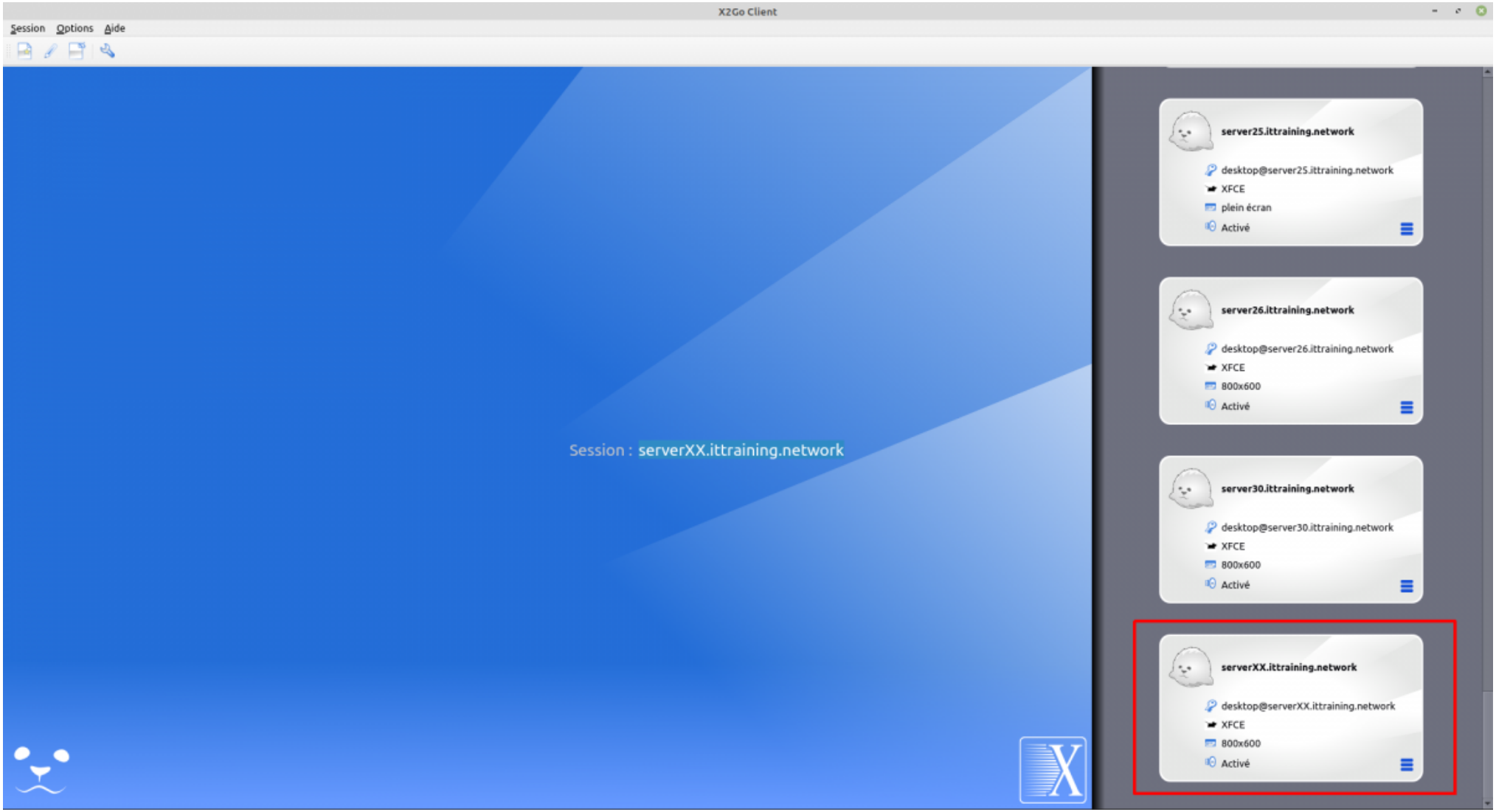
Naviguez au site **https://wiki.x2go.org/doku.php/download:start** et téléchargez le client X2Go pour votre architecture (Linux, Windows™ ou macOS™):



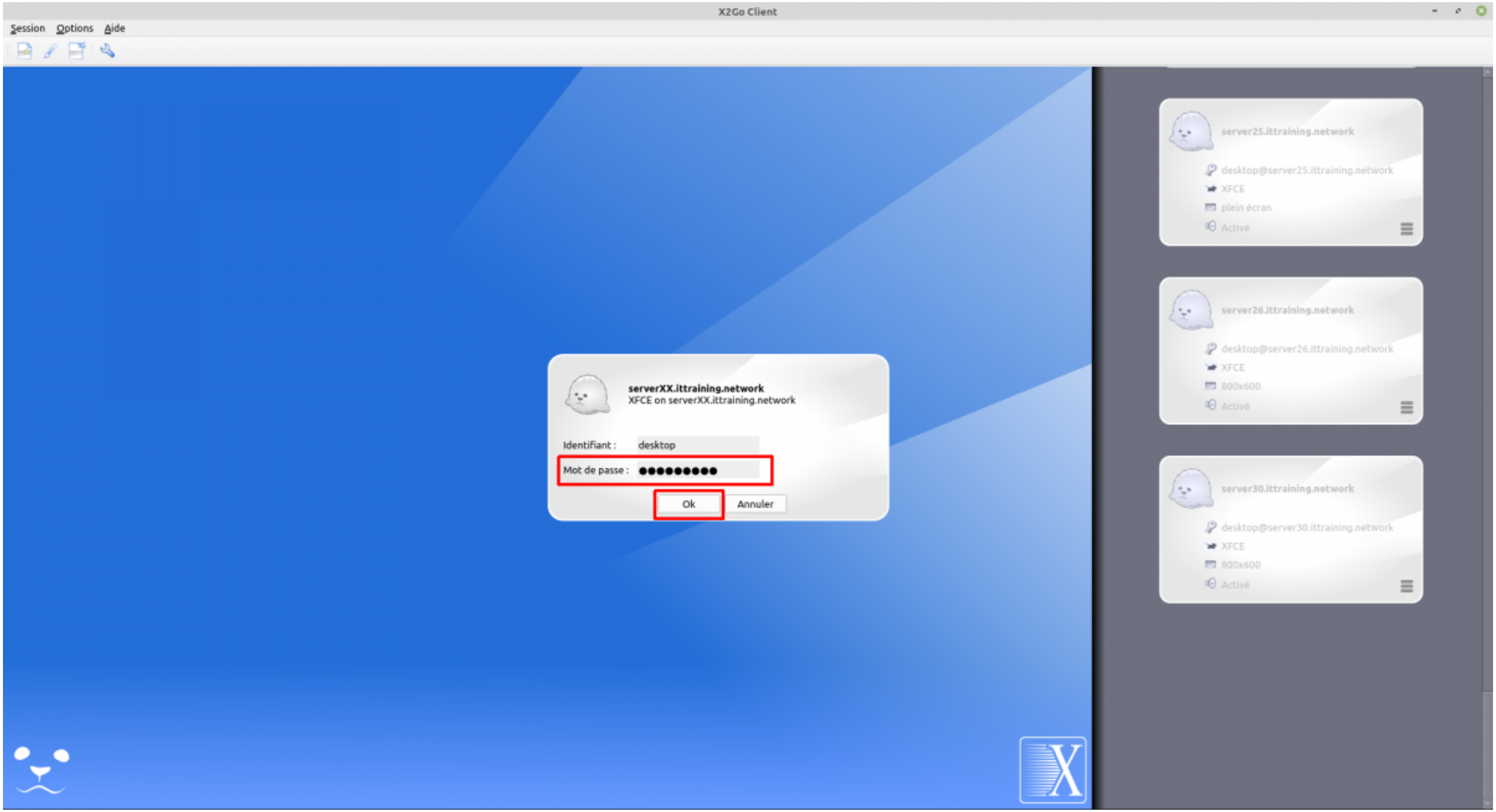
Installez le client, ouvrez l'application et créez une nouvelle session en **remplaçant** la valeur **XX** par le **numéro du serveur** qui vous a été communiqué par votre formateur :



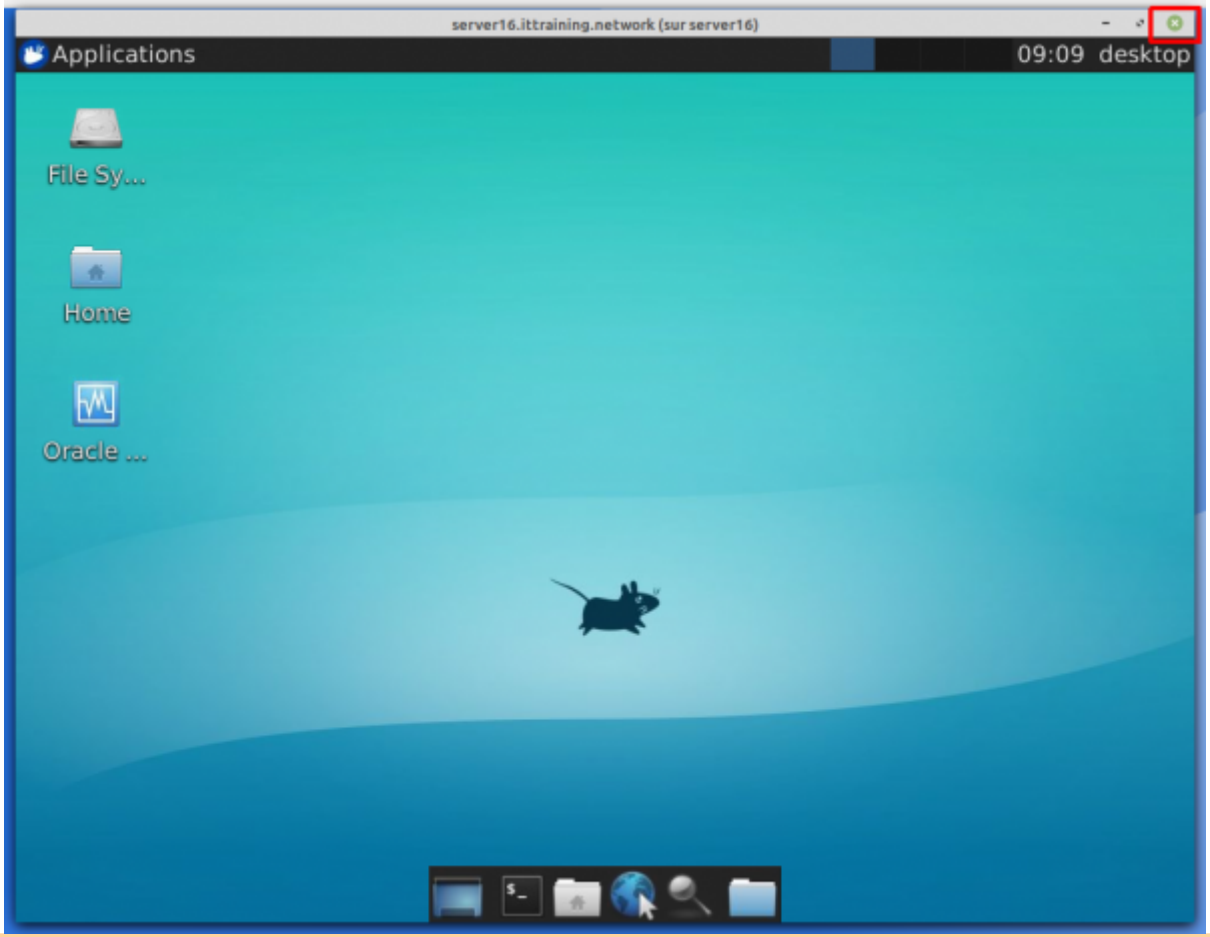
Vous verrez apparaître une boîte represantant votre nouvelle connexion à droite de l'écran :



Cliquez sur cette boîte puis renseignez le mot de passe de votre serveur dans le cloud et cliquez sur le bouton **ok** :



A l'issu de quelques minutes vou aurez accès à votre serveur dans le cloud en mode graphique :

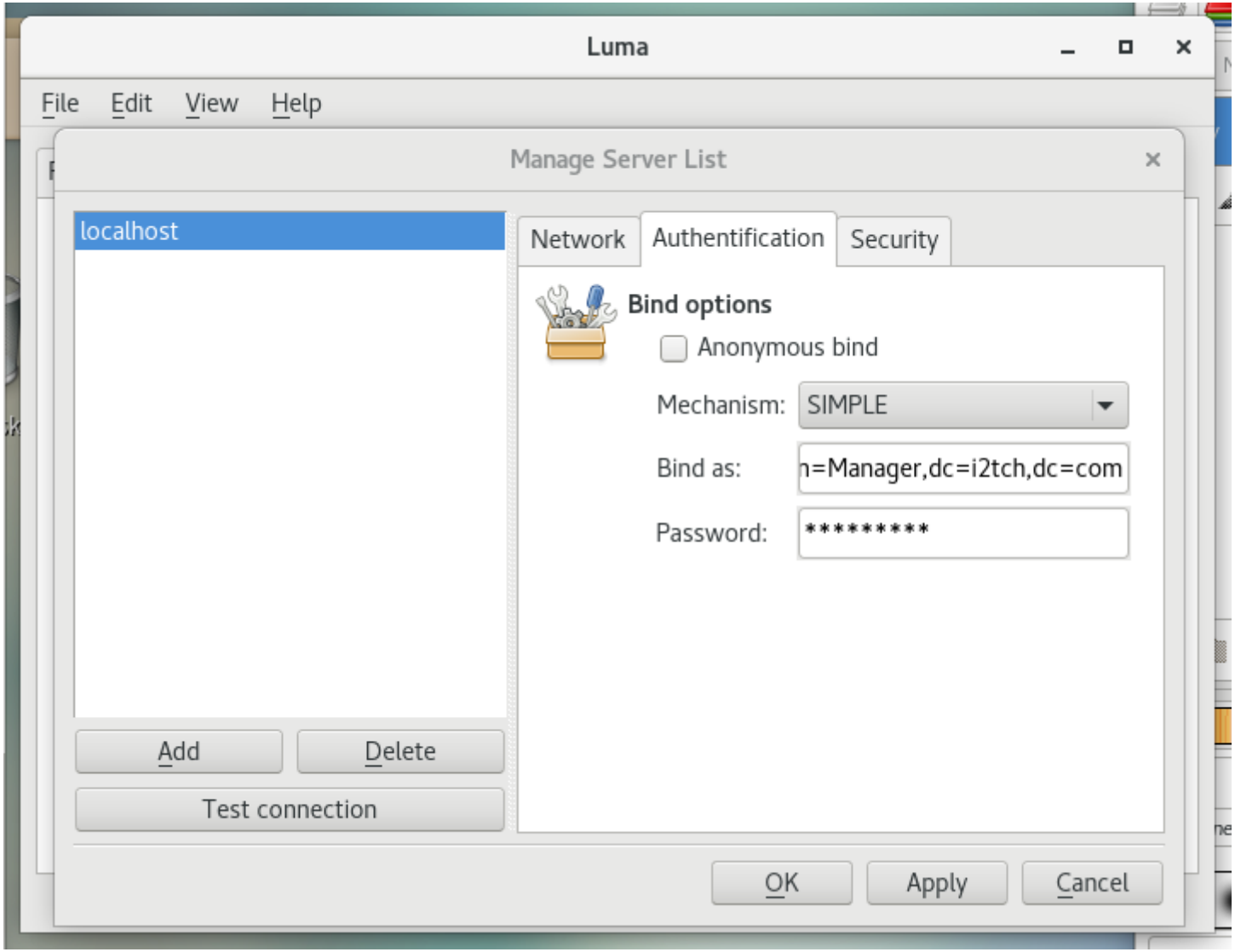


Important - Quand vous quittez votre serveur cloud, NE l'éteignez PAS. Cliquez simplement sur la croix en haut à droite de la fenêtre pour la fermer.

Dans l'interface de votre connexion graphique à votre serveur, ouvrez VirtualBox puis double-cliquez sur la VM CentOS_7. Dans la fenêtre qui s'ouvre, connectez-vous à votre VM CentOS_7 en tant que **trainee** en utilisant le mot de passe **trainee**.

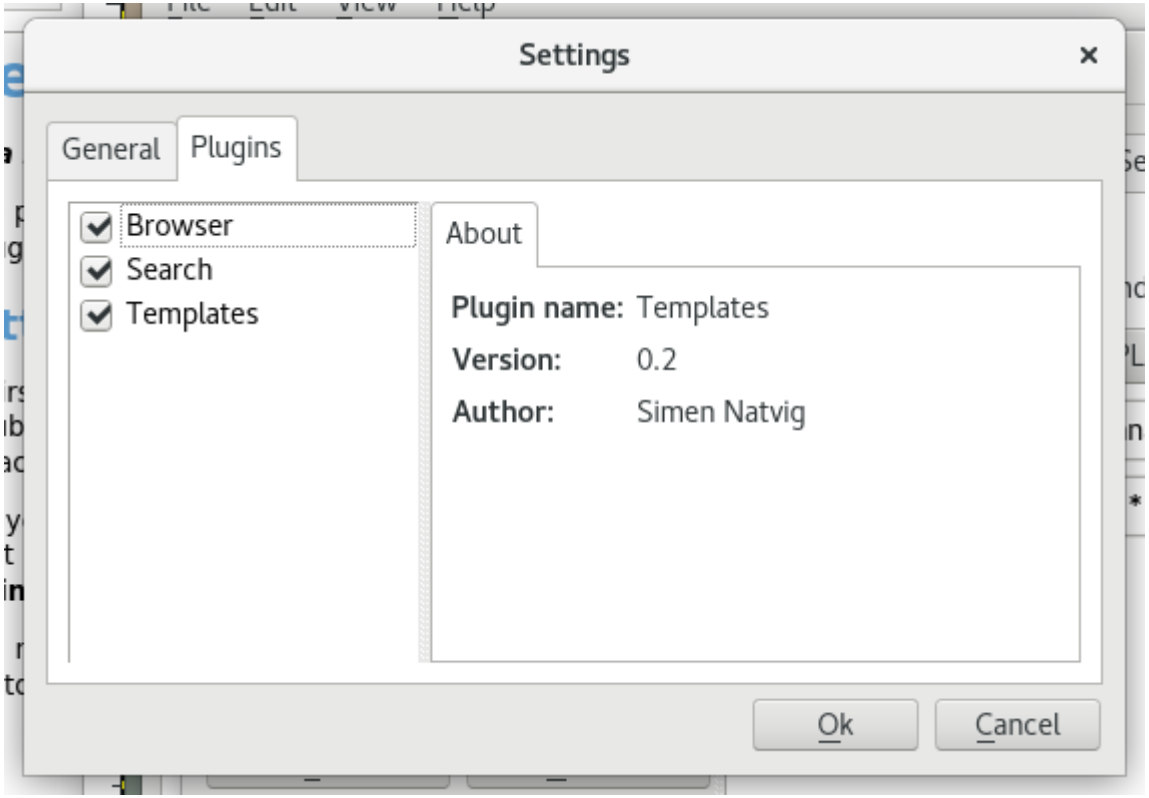
Lancez luma via les menus **Applications > System Tools > Luma LDAP Browser**.

Connectez-vous à votre serveur LDAP en utilisant luma. Cliquez sur le menu **Edit > Server List**. Cliquez sur **Add** puis renseignez le nom localhost. Sélectionnez **Authentification**, décochez **Anonymous bind** et remplissez les champs pour une connexion **simple** :

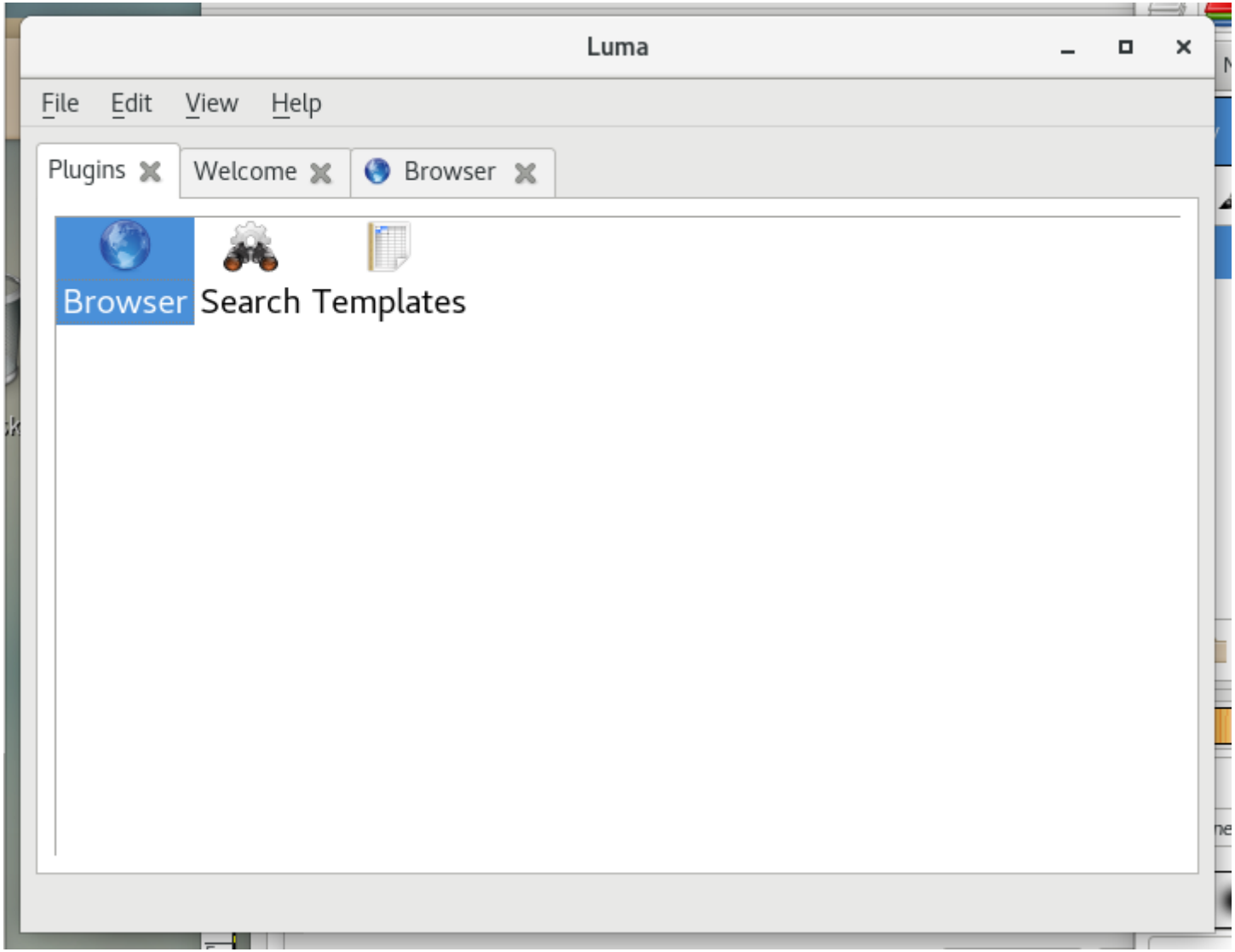


Cliquez sur le bouton **Apply** puis sur le bouton **Ok**.

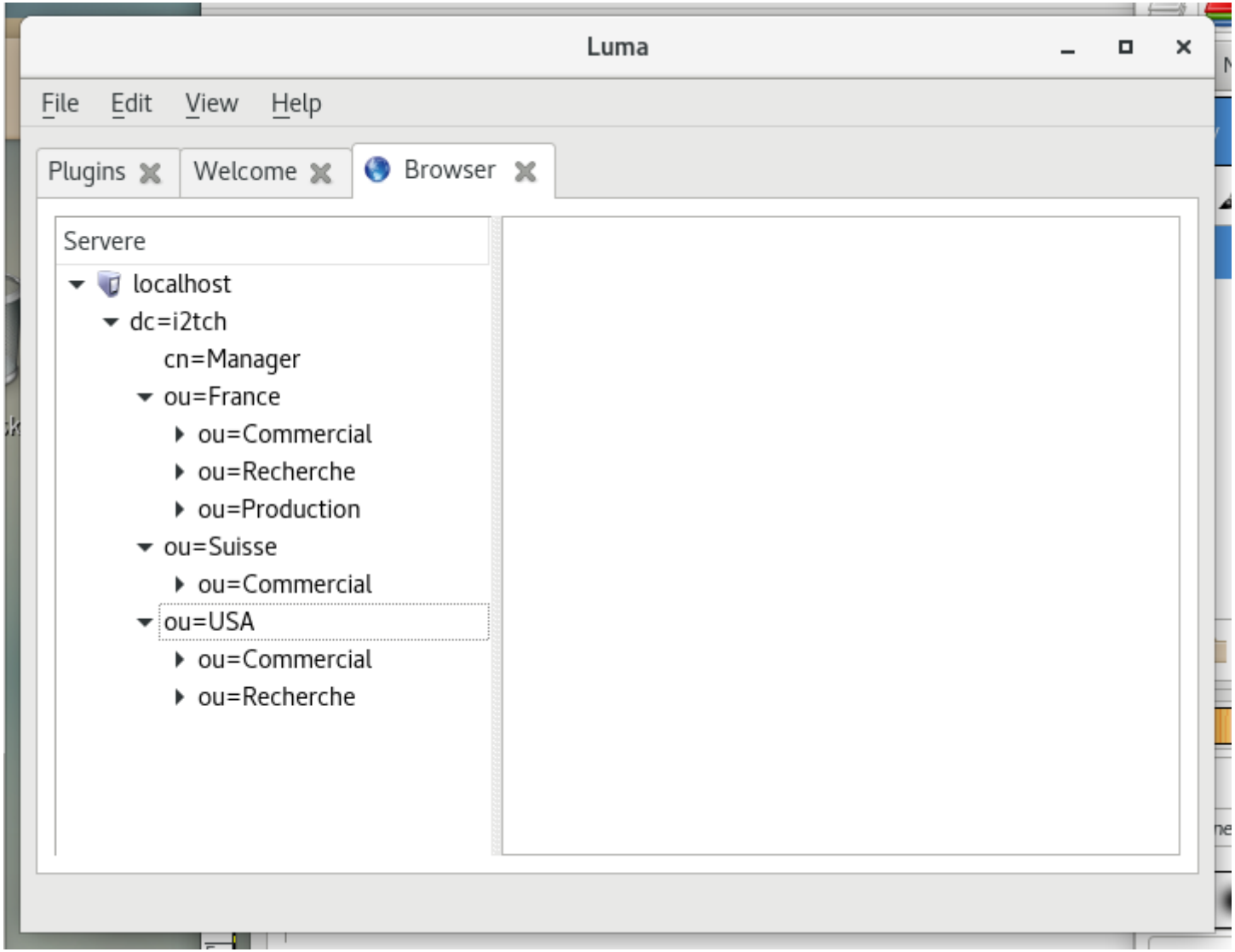
Cliquez sur l'onglet **Plugins** et cochez tout. Cliquez ensuite sur le bouton **Ok** :



Double-cliquez sur **Browser** :



Cliquez sur **localhost**. Vous obtiendrez un résultat similaire à celui-ci :



Le Directory Information Tree

Ce que vous pouvez constater avec ces deux outils est la présence du DIT (**D**irectory **I**nformation **T**ree). Ce DIT contient des **entrées** ayant des

attributs dont les principaux types sont :

Noeud	Nom	Description
dc	domain component	domaine internet
c	country	pays
o	organization	organisation
ou	organizational unit	unité d'organisation
cn	common name	nom

Il est possible de faire référence à un entrée en utilisant un de deux noms :

Nom	Abréviation	Exemple
Distinguished Name	DN	ou=Commercial,ou=Suisse,dc=fenestros,dc=com
Relative Distinguished Name	RDN	ou=Commercial

Vous noterez qu'il existe trois entrées ayant le même **RDN** :

RDN	DN
ou=Commercial	ou=Commercial,ou=France,dc=fenestros,dc=com
ou=Commercial	ou=Commercial,ou=Suisse,dc=fenestros,dc=com
ou=Commercial	ou=Commercial,ou=USA,dc=fenestros,dc=com

Comme démontre cet exemple, il n'y a pas de contraintes au niveau des noms *à l'excéption de l'unicité* du DN.

Les noms des entités sont codés en UTF-8. Ceci implique que les noms peuvent contenir n'importe quelle combinaison de caractères y compris des éspaces.

Les alias

Le DIT peut également comporter des **alias** - des noeuds qui pointent vers une autre entrée du DIT.

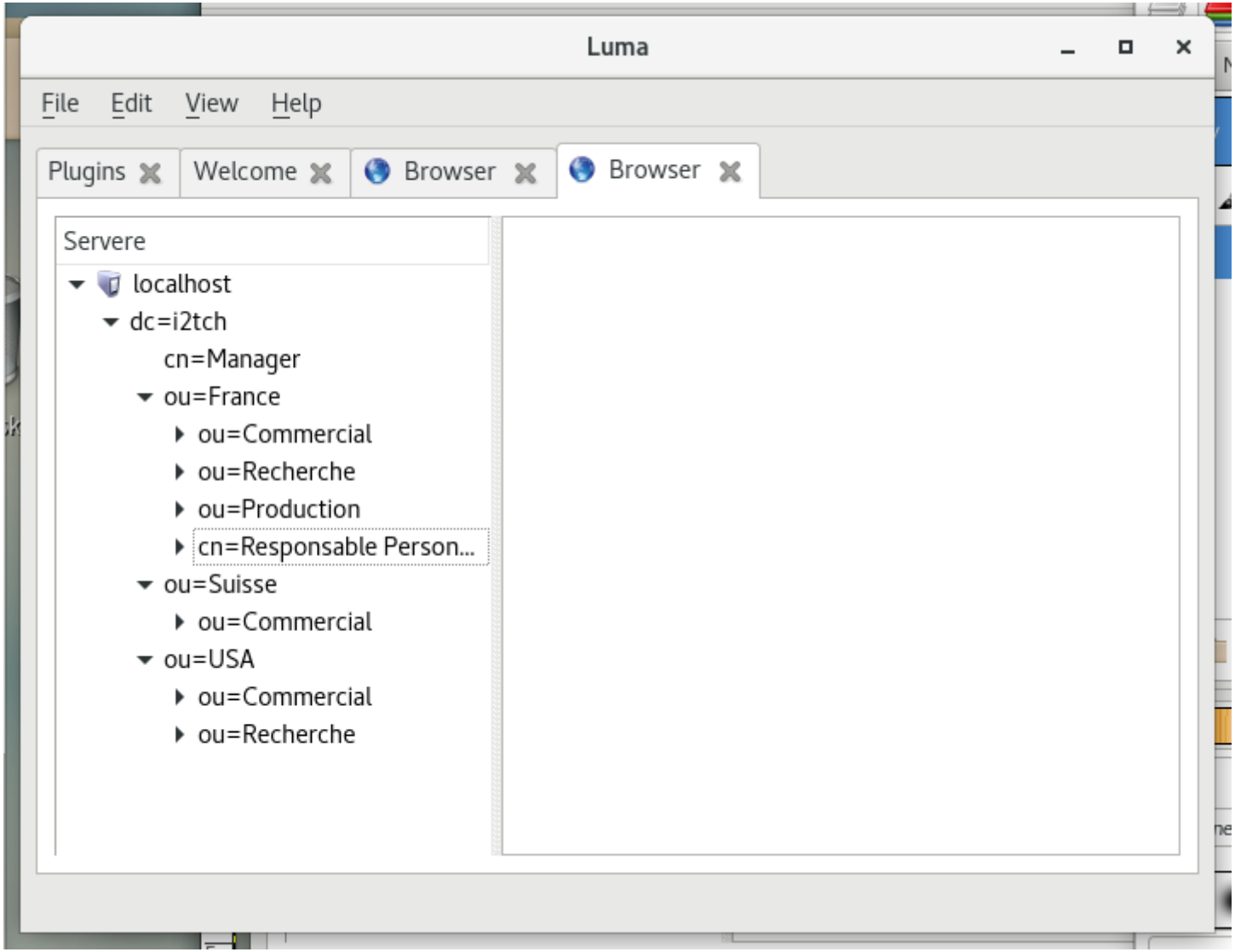
Pour illustrer ce point, créez le fichier LDIF **alias.ldif** et éditez-le ainsi :

```
[root@centos7 luma-master]# cd ~
[root@centos7 ~]# vi alias.ldif
[root@centos7 ~]# cat alias.ldif
version: 1
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

Importez maintenant le fichier LDIF dans le DIT :

```
[root@centos7 ~]# ldapadd -f alias.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=Responsable Personnel,ou=France,dc=i2tch,dc=com"
```

Constatez maintenant le résultat :



Notez que le noeud vers lequel pointe l'alias n'existe pas.

Créez le fichier LDIF **directeur.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi directeur.ldif
```

```
[root@centos7 ~]# cat directeur.ldif
version: 1
dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
```

Créez donc l'entrée **directeur** en utilisant le fichier **directeur.ldif** :

```
[root@centos7 ~]# ldapadd -f directeur.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=directeur,ou=France,dc=i2tch,dc=com"
ldap_add: Server is unwilling to perform (53)
    additional info: no global superior knowledge
```

Important - Cette erreur indique que OpenLDAP ne sait pas où mettre les données. Ceci est causé par le fait que le schéma adéquat n'a pas été chargé.

Modifiez donc votre fichier slapd.ldif en ajoutant les lignes suivantes :

```
[root@centos7 ~]# vi slapd.ldif
[root@centos7 ~]# cat slapd.ldif
...
include: file:///etc/openldap/schema/core.ldif
include: file:///etc/openldap/schema/corba.ldif
include: file:///etc/openldap/schema/cosine.ldif
include: file:///etc/openldap/schema/duaconf.ldif
include: file:///etc/openldap/schema/dyngroup.ldif
include: file:///etc/openldap/schema/inetorgperson.ldif
```

```
include: file:///etc/openldap/schema/java.ldif
include: file:///etc/openldap/schema/misc.ldif
include: file:///etc/openldap/schema/nis.ldif
include: file:///etc/openldap/schema/openldap.ldif
include: file:///etc/openldap/schema/ppolicy.ldif
include: file:///etc/openldap/schema/collective.ldif
...
```

Arrêtez le serveur slapd :

```
[root@centos7 ~]# systemctl stop slapd
```

Re-créez la base de données de la configuration :

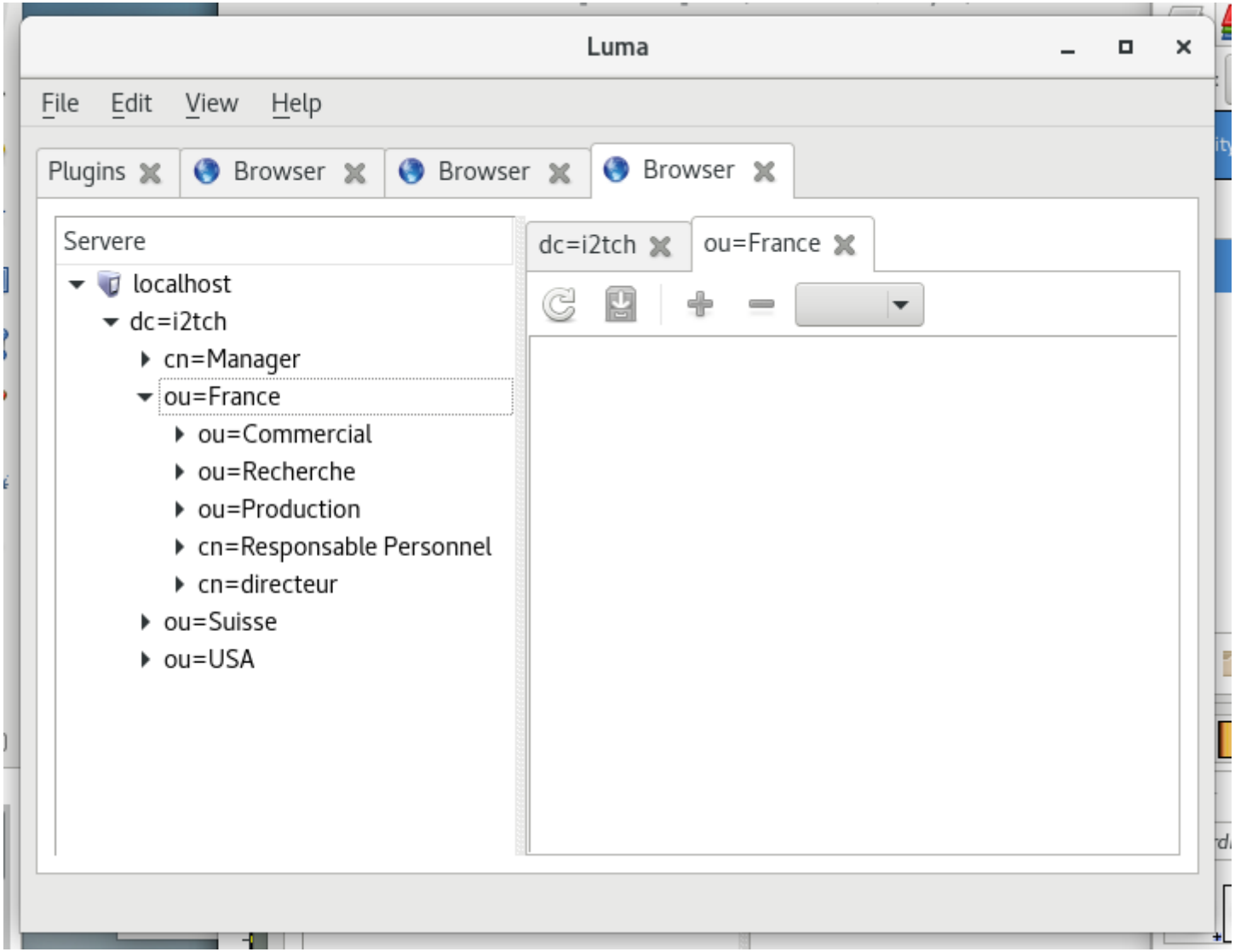
```
[root@centos7 ~]# rm -rf /etc/openldap/slapd.d/*
[root@centos7 ~]# ls /etc/openldap/slapd.d
[root@centos7 ~]# slapadd -F /etc/openldap/slapd.d -n 0 -l slapd.ldif
_################### 100.00% eta   none elapsed            none fast!
Closing DB...
[root@centos7 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos7 ~]# ls -lR /etc/openldap/slapd.d
/etc/openldap/slapd.d:
total 8
drwxr-x---. 3 ldap ldap 4096 Jan 10 10:46 cn=config
-rw-------. 1 ldap ldap  627 Jan 10 10:46 cn=config.ldif

/etc/openldap/slapd.d/cn=config:
total 24
drwxr-x---. 2 ldap ldap 4096 Jan 10 10:46 cn=schema
-rw-------. 1 ldap ldap  378 Jan 10 10:46 cn=schema.ldif
-rw-------. 1 ldap ldap  513 Jan 10 10:46 olcDatabase={0}config.ldif
-rw-------. 1 ldap ldap  443 Jan 10 10:46 olcDatabase={-1}frontend.ldif
-rw-------. 1 ldap ldap  558 Jan 10 10:46 olcDatabase={1}monitor.ldif
-rw-------. 1 ldap ldap  666 Jan 10 10:46 olcDatabase={2}hdb.ldif
```

```
/etc/openldap/slapd.d/cn=config/cn=schema:
total 76
-rw-------. 1 ldap ldap 15578 Jan 10 10:46 cn={0}core.ldif
-rw-------. 1 ldap ldap  3845 Jan 10 10:46 cn={10}ppolicy.ldif
-rw-------. 1 ldap ldap  1523 Jan 10 10:46 cn={11}collective.ldif
-rw-------. 1 ldap ldap  1283 Jan 10 10:46 cn={1}corba.ldif
-rw-------. 1 ldap ldap 11363 Jan 10 10:46 cn={2}cosine.ldif
-rw-------. 1 ldap ldap  4489 Jan 10 10:46 cn={3}duaconf.ldif
-rw-------. 1 ldap ldap  1693 Jan 10 10:46 cn={4}dyngroup.ldif
-rw-------. 1 ldap ldap  2857 Jan 10 10:46 cn={5}inetorgperson.ldif
-rw-------. 1 ldap ldap  2589 Jan 10 10:46 cn={6}java.ldif
-rw-------. 1 ldap ldap  1519 Jan 10 10:46 cn={7}misc.ldif
-rw-------. 1 ldap ldap  6495 Jan 10 10:46 cn={8}nis.ldif
-rw-------. 1 ldap ldap  1290 Jan 10 10:46 cn={9}openldap.ldif
[root@centos7 ~]# slaptest -u
config file testing succeeded

[root@centos7 ~]# systemctl start slapd
```

Créez donc l'entrée **directeur** en utilisant le fichier **directeur.ldif** :

```
[root@centos7 ~]# ldapadd -f directeur.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=directeur,ou=France,dc=i2tch,dc=com"
```

Revenez à Luma. Vous obtiendrez une fenêtre similaire à celle-ci :



Créez le maintenant fichier LDIF **plus.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi plus.ldif
[root@centos7 ~]# cat plus.ldif
version: 1
```

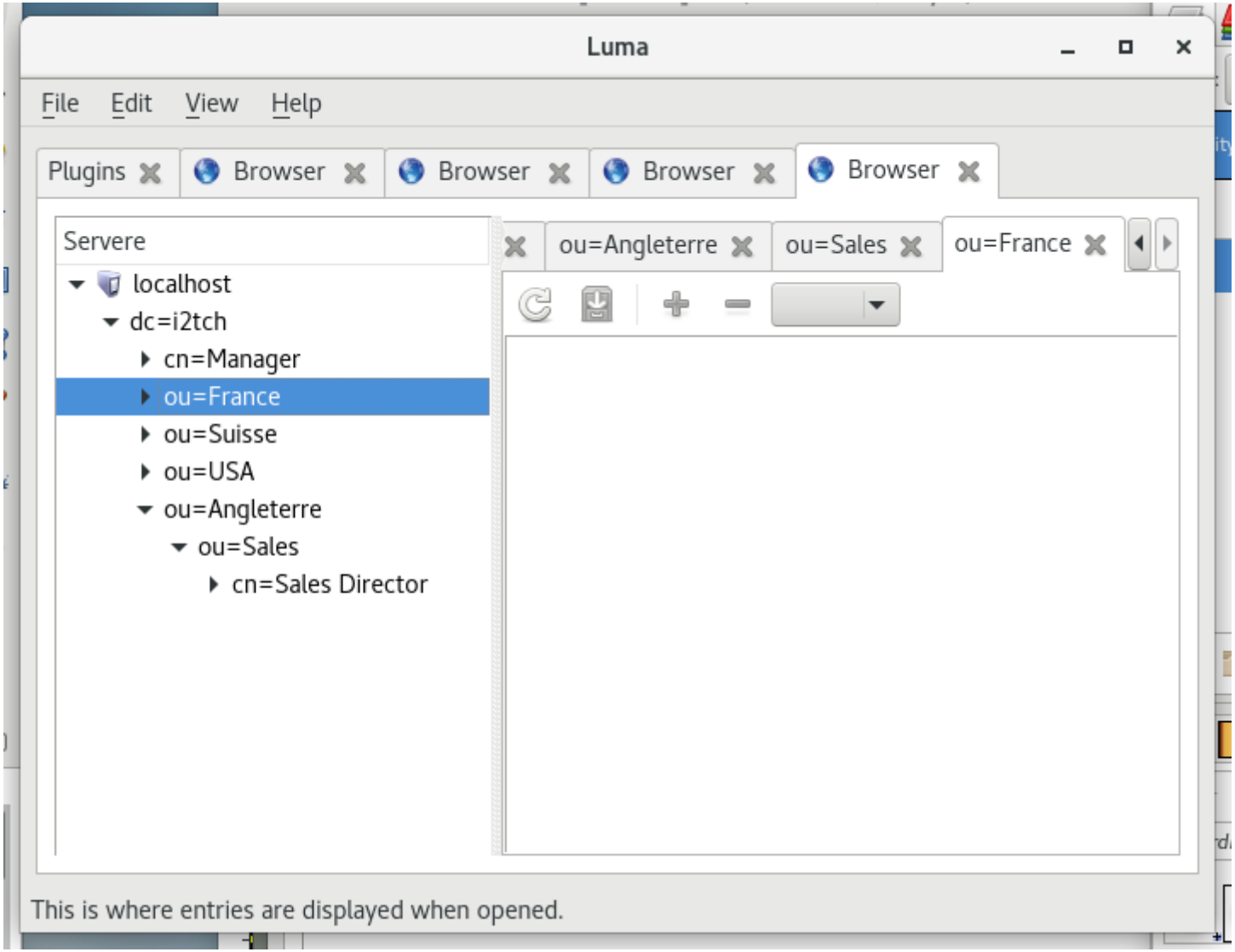
```
dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont
```

Créez donc les entrées en utilisant le fichier **plus.ldif** :

```
[root@centos7 ~]# ldapadd -f plus.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "ou=Angleterre,dc=i2tch,dc=com"

adding new entry "ou=Sales,ou=Angleterre,dc=i2tch,dc=com"
```

```
adding new entry "cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com"

adding new entry "cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com"

adding new entry "cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

Revenez à Luma.Vous obtiendrez une fenêtre similaire à celle-ci :



1.2 - Installation et Utilisation du Client HTML phpLDAPadmin

Commencez par installer phpLDAPadmin :

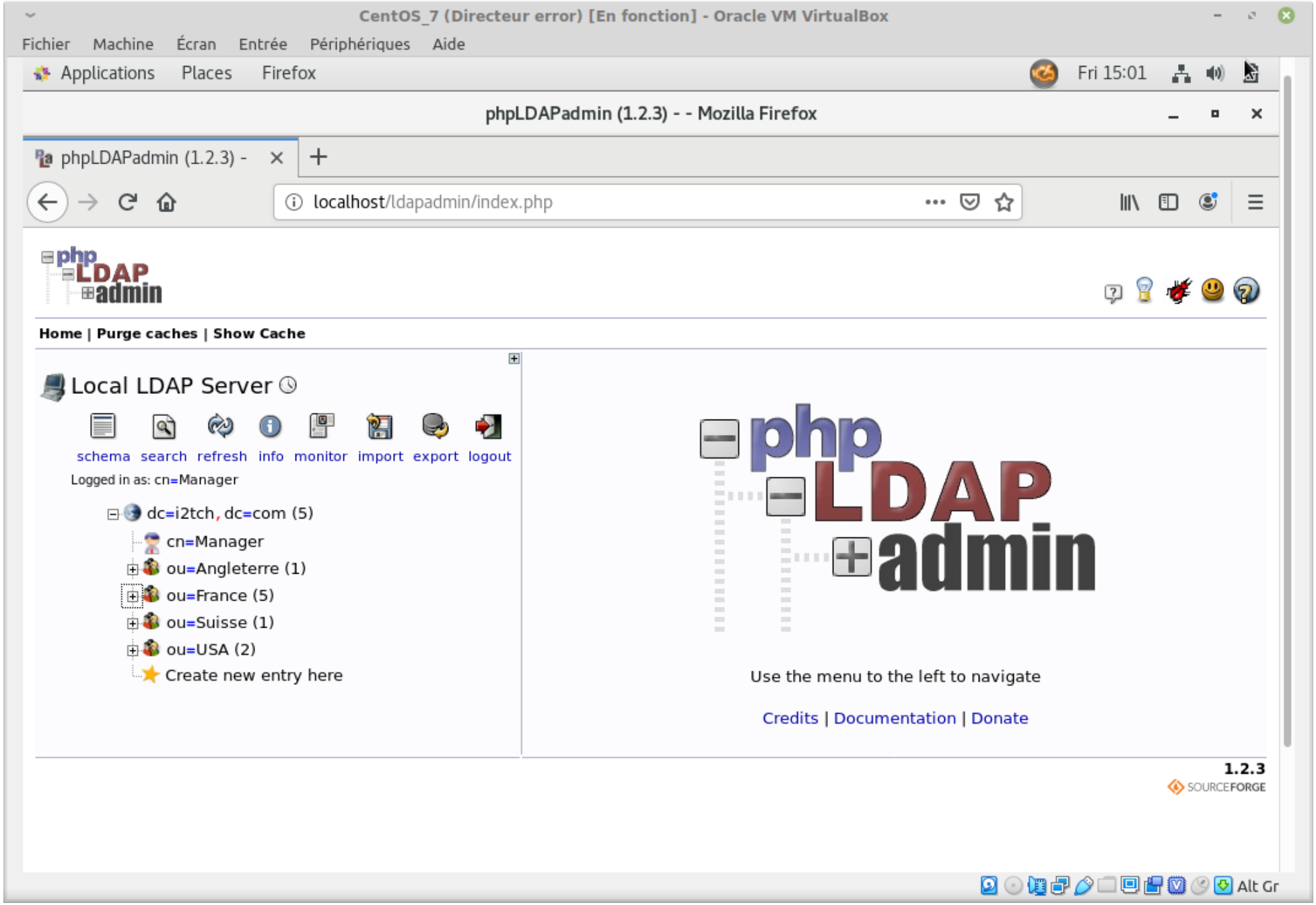
```
[root@centos7 ~]# yum -y install httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[root@centos7 ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
[root@centos7 ~]# systemctl start httpd
[root@centos7 ~]# yum -y install php php-mbstring php-pear php-ldap
[root@centos7 ~]# yum -y install epel-release
[root@centos7 ~]# yum -y install phpldapadmin
[root@centos7 ~]# systemctl restart httpd
```

Modifiez les lignes **332**, **388**, **397** et **398** du fichier **/etc/phpldapadmin/config.php** :

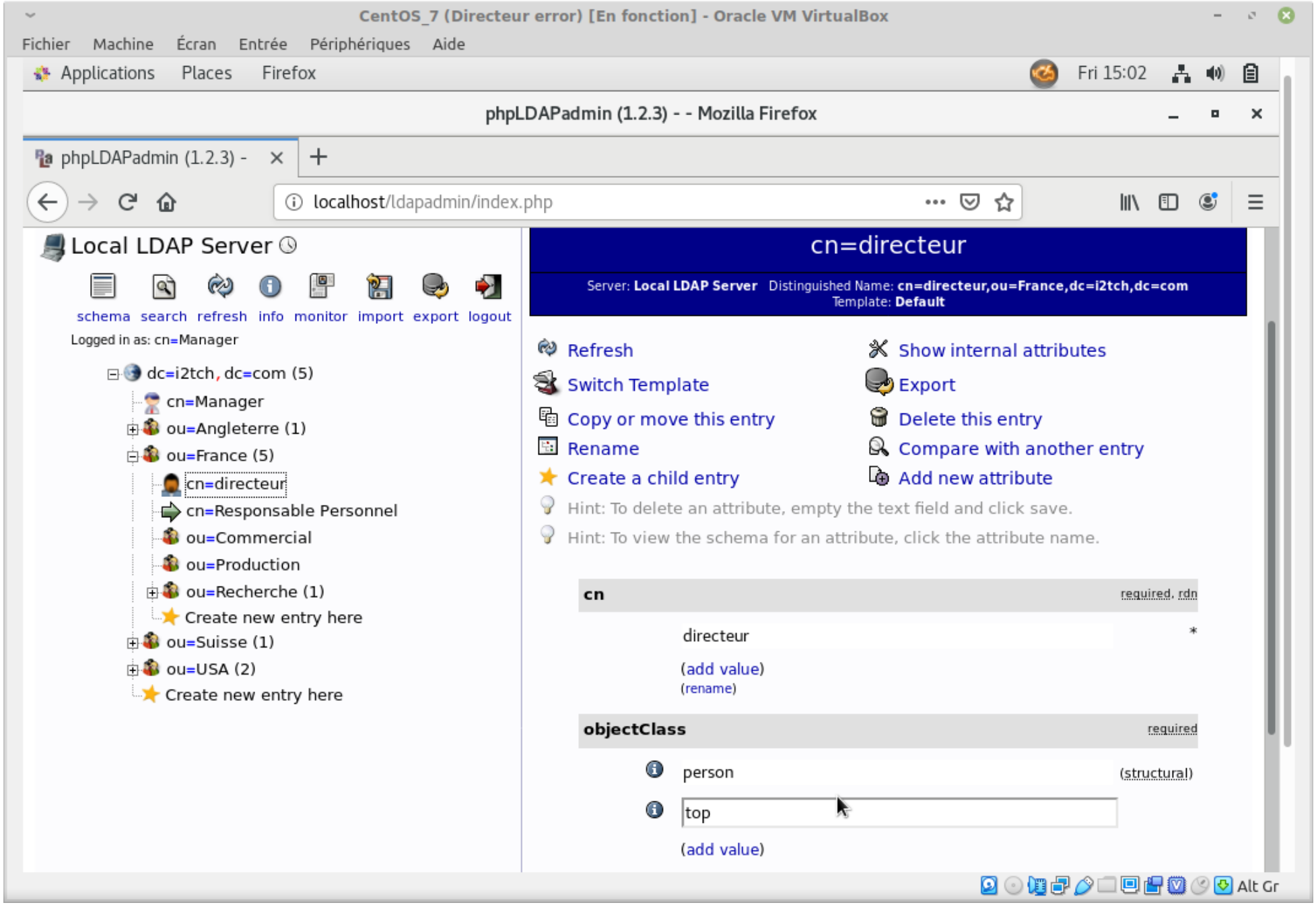
```
[root@centos7 ~]# vi /etc/phpldapadmin/config.php
[root@centos7 ~]# cat /etc/phpldapadmin/config.php
...
    332 $servers->setValue('login','bind_id','cn=Manager,dc=i2tch,dc=com');
    ...
    388 $servers->setValue('appearance','pla_password_hash','ssha');

    397 $servers->setValue('login','attr','dn');
    398 // $servers->setValue('login','attr','uid');
...
```

Les attributs

Dans le navigateur web de la **machine virtuelle** rendez-vous à l'URL **http://localhost/ldapadmin** et connectez-vous :

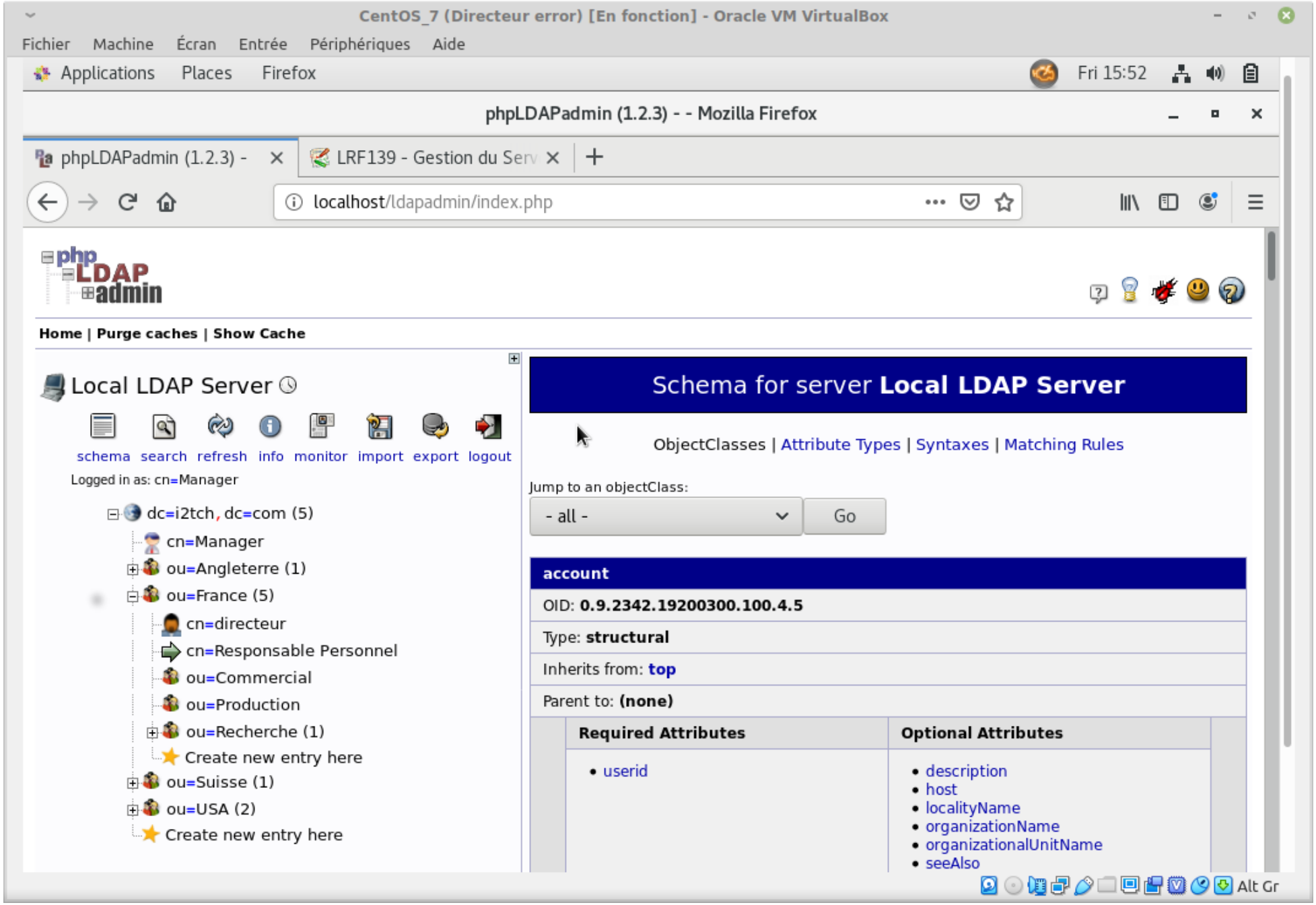

CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Fri 15:01
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/index.php
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
ou=Suisse (1)
ou=USA (2)
Create new entry here
Use the menu to the left to navigate
Credits | Documentation | Donate
1.2.3
SOURCEFORGE
Alt Gr

Regardons maintenant l'entrée du **directeur** en France et plus spécifiquement les **attributs** :

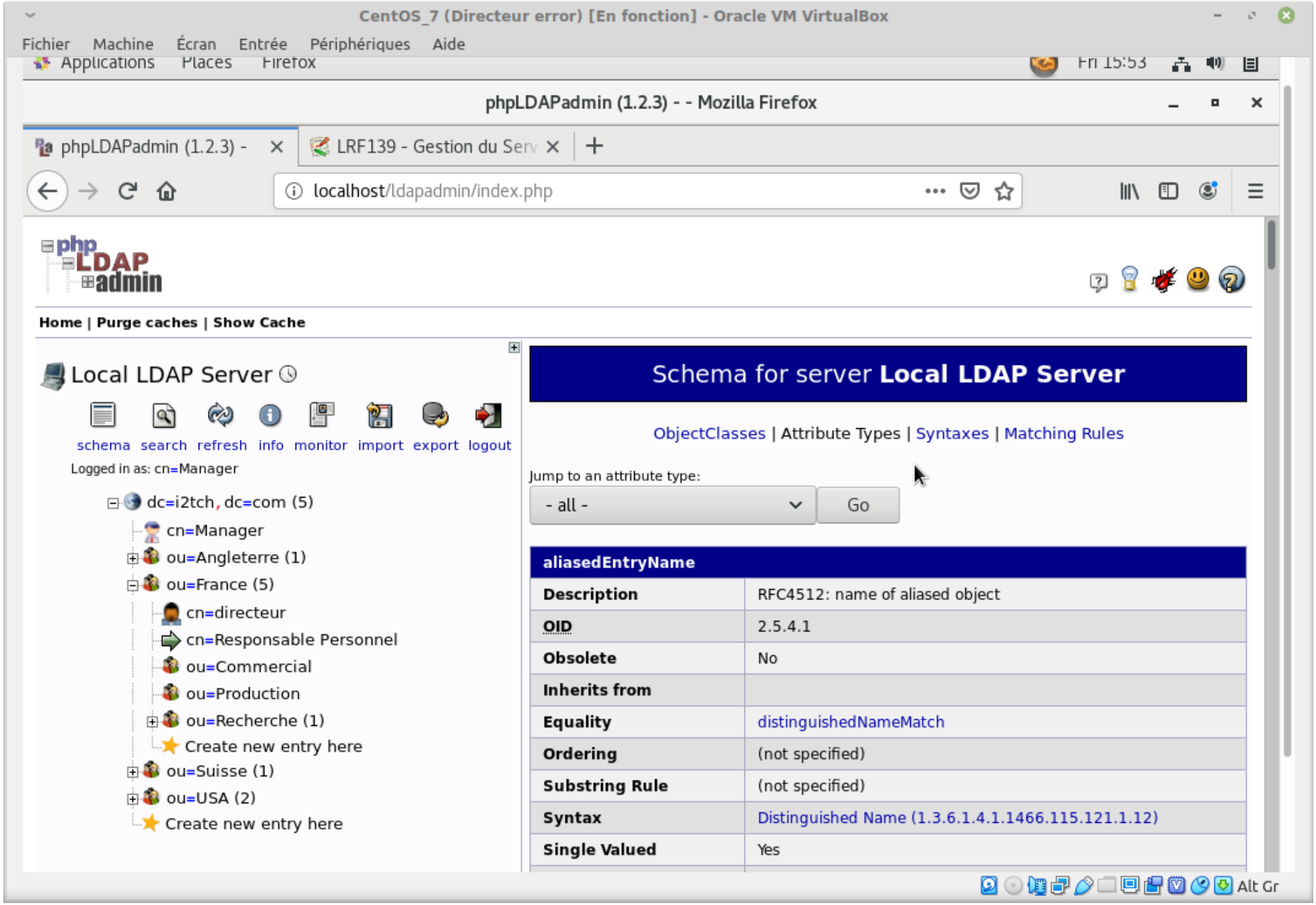

CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Fri 15:02
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/index.php
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
cn=directeur
Server: Local LDAP Server Distinguished Name: cn=directeur,ou=France,dc=i2tch,dc=com
Template: Default
Refresh
Show internal attributes
Switch Template
Export
Copy or move this entry
Delete this entry
Rename
Compare with another entry
Create a child entry
Add new attribute
Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.
cn
required, rdn
directeur
*
(add value)
(rename)
objectClass
required
person
(structural)
top
(add value)
Alt Gr

On peut constater la présence de trois attributs, certains apparaissent en plusieurs exemples.

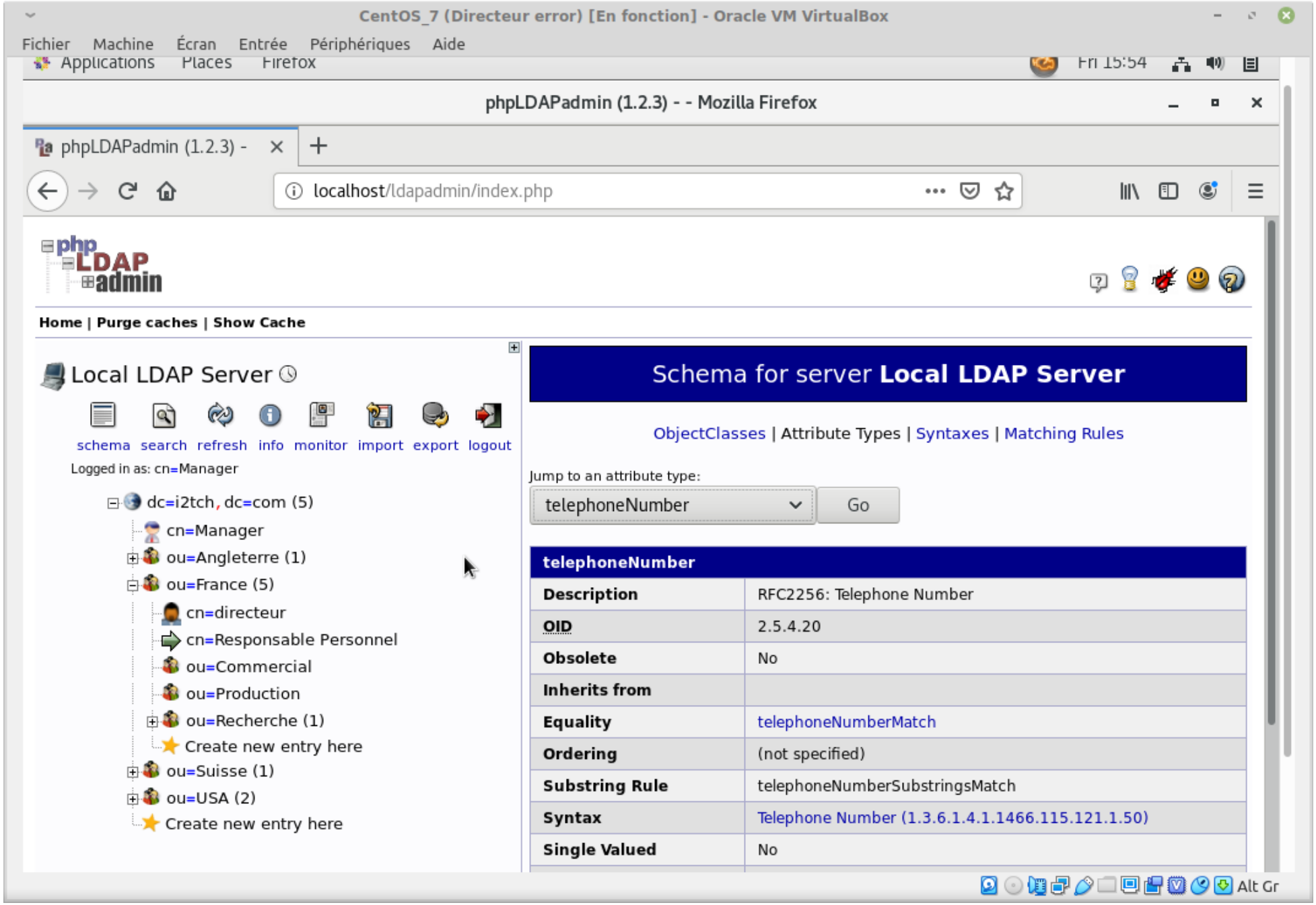
Cliquez sur l'icone **schema** :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Fri 15:52
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
LRF139 - Gestion du Serv
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an objectClass:
- all -
Go
account
OID: 0.9.2342.19200300.100.4.5
Type: structural
Inherits from: top
Parent to: (none)
Required Attributes
userid
Optional Attributes
description
host
localityName
organizationName
organizationalUnitName
seeAlso
Alt Gr

Dans le panneau de droite, cliquez sur le lien **Attribute Types** :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Fri 15:53
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
LRF139 - Gestion du Serv
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an attribute type:
- all -
Go
aliasedEntryName
Description RFC4512: name of aliased object
OID 2.5.4.1
Obsolete No
Inherits from
Equality distinguishedNameMatch
Ordering (not specified)
Substring Rule (not specified)
Syntax Distinguished Name (1.3.6.1.4.1.1466.115.121.1.12)
Single Valued Yes
Alt Gr

Dans la liste déroulante, choisissez l'attribut **telephoneNumber** :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Fri 15:54
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an attribute type:
telephoneNumber
Go
telephoneNumber
Description RFC2256: Telephone Number
OID 2.5.4.20
Obsolete No
Inherits from
Equality telephoneNumberMatch
Ordering (not specified)
Substring Rule telephoneNumberSubstringsMatch
Syntax Telephone Number (1.3.6.1.4.1.1466.115.121.1.50)
Single Valued No
Alt Gr

Chaque attribut est défini par plusieurs *types*. Dans le cas du **telephoneNumber**, nous trouvons :

Type	**Nom français**	**Description**
EQUALITY	Egalité	Règles d'égalités
OID	Identifiant de l'objet	Object Identifier
SYNTAX	Syntaxe	OID de ce que peut contenir l'attribut

Les **OID** sont standardisés. Vous pouvez chercher un OID sur le site Internet http://www.oid-info.com/.

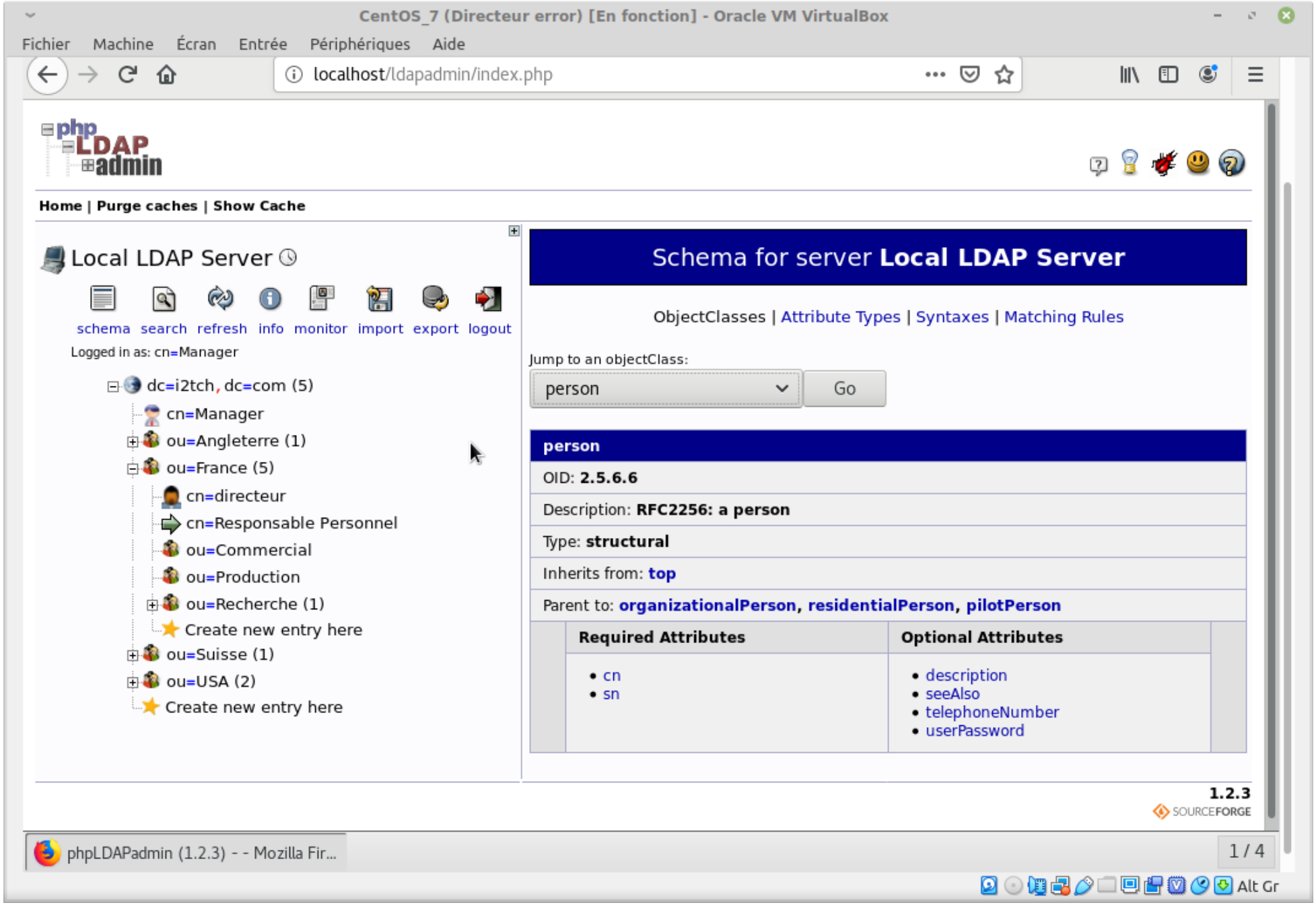
Un attribut peut dériver d'un autre attribut. Cet héritage implique le respect des caractéristiques de l'attribut parent. Dans ce cas l'héritage est défini par l'attribut **SUP** dont la valeur est le nom de l'attribut parent.

Le serveur gère certains attributs automatiquement. Ces attributs sont appelés **attributs opérationnels**, par exemple :

Attributs Opérationnel	**Exemple**
createTimestamp	20080606075042Z
modifyTimestamp	20080606075042Z
creatorsName	cn=Manager,dc=i2tch,dc=com
modifiersName	cn=Manager,dc=i2tch,dc=com

Les classes

Chaque entrée dans le DIT **doit** comporter au moins **un** attribut **objectClass**. La classe d'objet du directeur est **person**. Dans le panneau de droite, cliquez sur le lien **ObjectClasses** et trouvez la classe **Person** dans la liste déroulante :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an objectClass:
person
Go
person
OID: 2.5.6.6
Description: RFC2256: a person
Type: structural
Inherits from: top
Parent to: organizationalPerson, residentialPerson, pilotPerson
Required Attributes
cn
sn
Optional Attributes
description
seeAlso
telephoneNumber
userPassword
1.2.3
SOURCEFORGE
phpLDAPadmin (1.2.3) - - Mozilla Fir...
1 / 4
Alt Gr

Dans cette fenêtre vous pouvez constater des Attributs nécessaires et des Attributs autorisés. En anglais ces deux termes correspondent à :

Elément	**Description**
MAY	Attributs autorisés
MUST	Attributs nécessaires

Notez aussi que cette classe est dite **STRUCTURAL**. Une entrée dans le DIT ne peut pas avoir plus d'une classe STRUCTURAL.

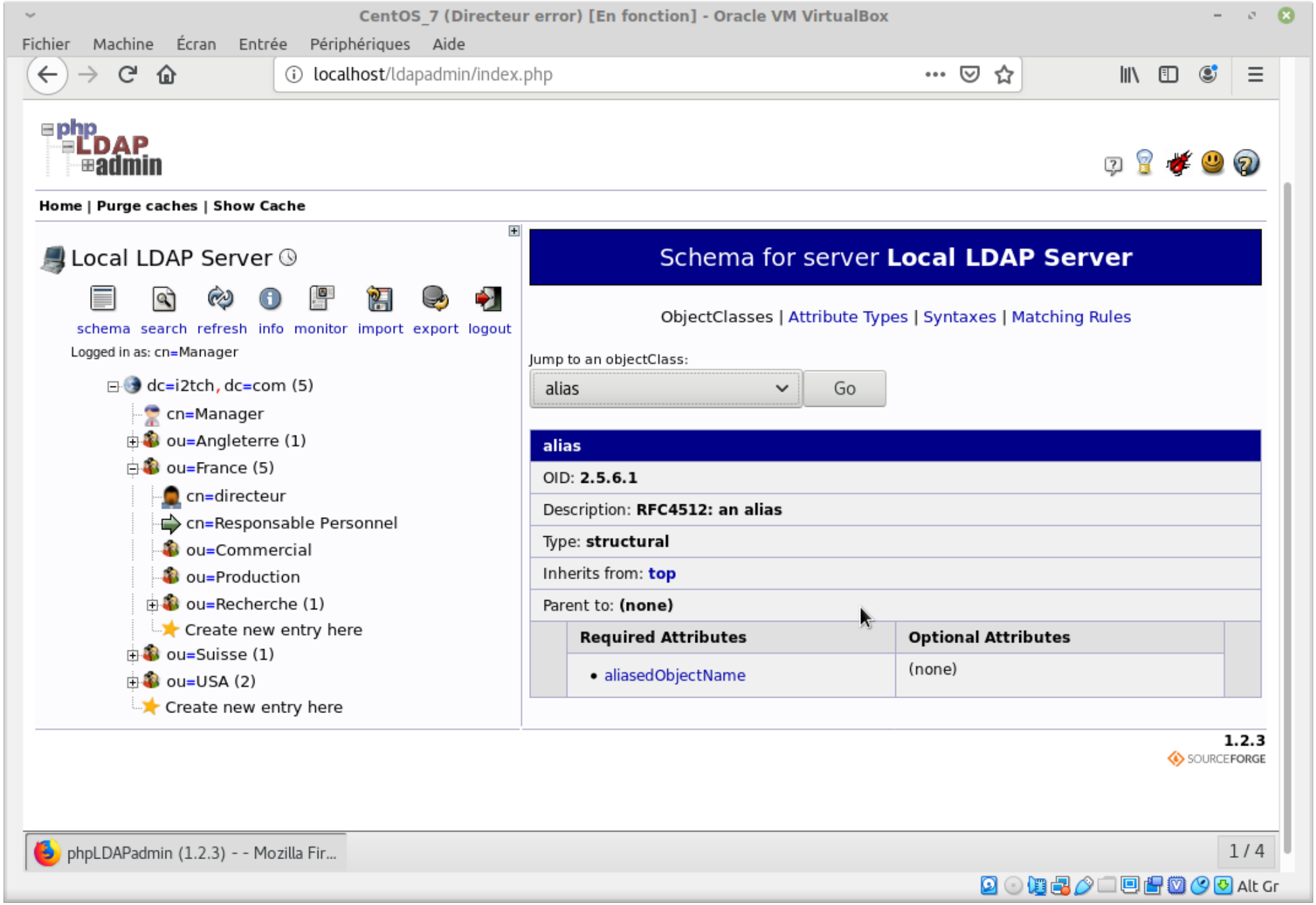
Le serveur OpenLDAP s'appuie sur trois types de classes d'objets :

- STRUCTURAL (STRUCTUREL)
- AUXILIARY (AUXILIAIRE)
- ABSTRACT (ABSTRAIT)

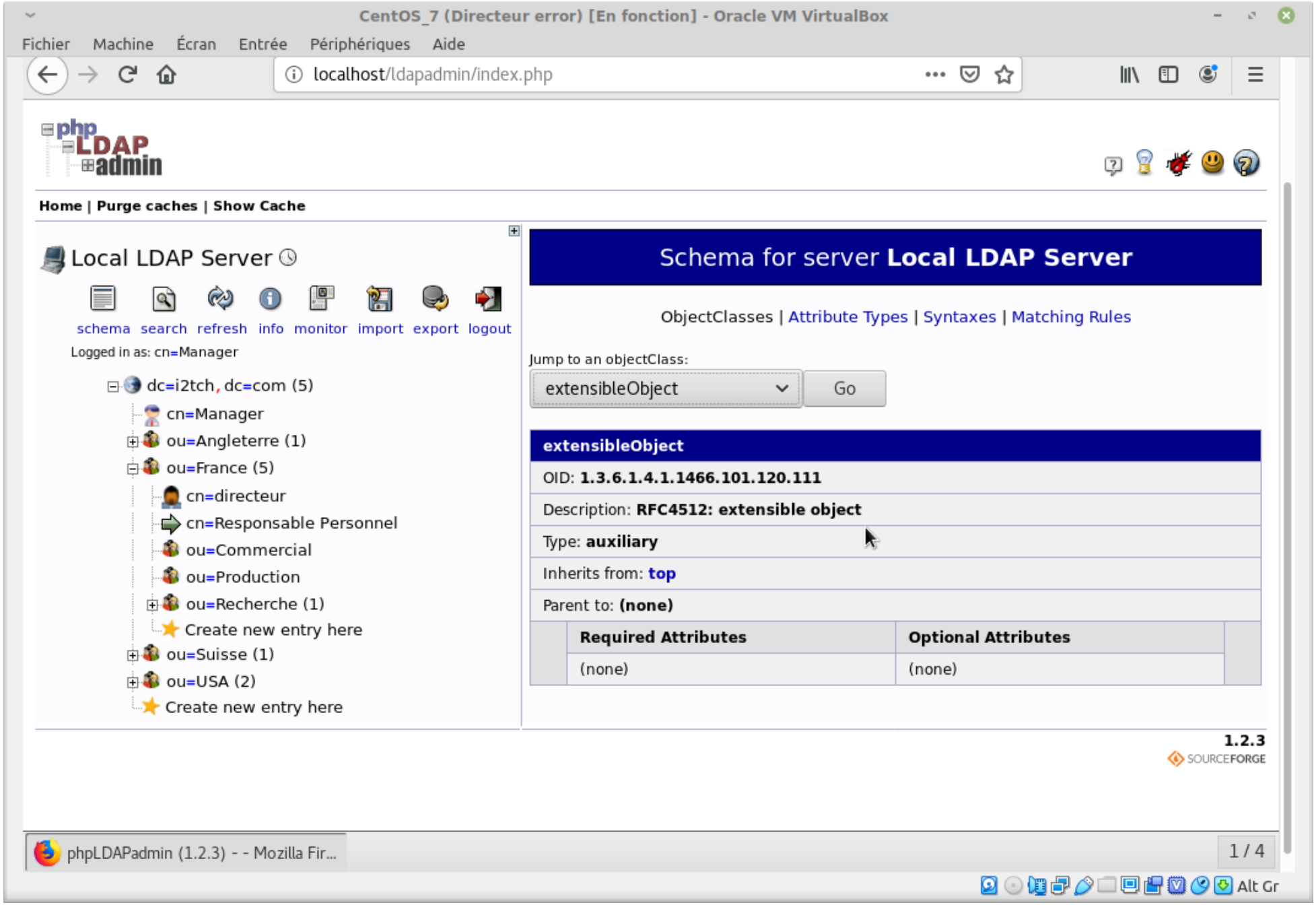
Prenons la cas de notre fichier LDIF **alias.ldif**. Notons que dans ce fichier, nous avions utilisé un objectClass **alias** :

```
version: 1
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
```

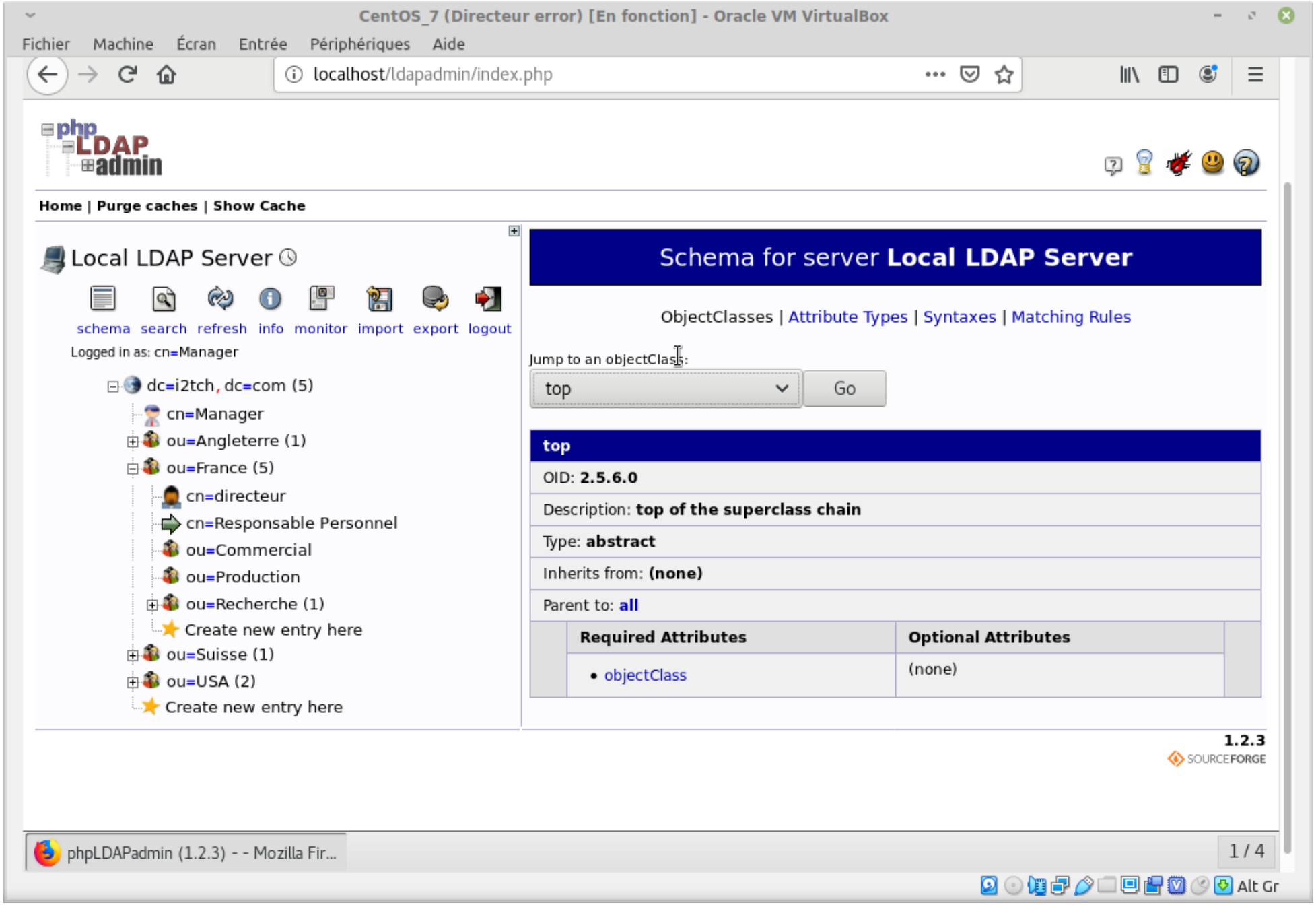
Si nous cherchons la définition de la classe alias, nous constatons que cette classe ne comprends pas d'attribut **cn** :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an objectClass:
alias
Go
alias
OID: 2.5.6.1
Description: RFC4512: an alias
Type: structural
Inherits from: top
Parent to: (none)
Required Attributes
Optional Attributes
aliasedObjectName
(none)
1.2.3
SOURCEFORGE
phpLDAPadmin (1.2.3) - - Mozilla Fir...
1 / 4
Alt Gr

L'utilisation de la classe auxiliaire **extensibleObject** a permis de créer l'attribut cn non défini dans la classe alias :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an objectClass:
extensibleObject
Go
extensibleObject
OID: 1.3.6.1.4.1.1466.101.120.111
Description: RFC4512: extensible object
Type: auxiliary
Inherits from: top
Parent to: (none)
Required Attributes
Optional Attributes
(none)
(none)
1.2.3
SOURCEFORGE
phpLDAPadmin (1.2.3) - - Mozilla Fir...
1 / 4
Alt Gr

Le dernier type de classe est **ABSTRACT**. La classe **top** est une classe ABSTRACT et chaque entrée de l'annuaire doit comporté une classe top :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
localhost/ldapadmin/index.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Schema for server Local LDAP Server
ObjectClasses | Attribute Types | Syntaxes | Matching Rules
Jump to an objectClass:
top
Go
top
OID: 2.5.6.0
Description: top of the superclass chain
Type: abstract
Inherits from: (none)
Parent to: all
Required Attributes
Optional Attributes
objectClass
(none)
1.2.3
SOURCEFORGE
phpLDAPadmin (1.2.3) - - Mozilla Fir...
1 / 4
Alt Gr

Les schémas

L'ensemble des attributs et des classes d'un annuaire porte le nom de **schéma**. Les schémas sont normalisés. Les fichiers de schémas sont stockés dans le répertoire **/etc/openldap/schema/** :

```
[root@centos7 ~]# ls /etc/openldap/schema/
collective.ldif    corba.schema  cosine.ldif    duaconf.schema   inetorgperson.ldif    java.schema  nis.ldif
openldap.schema  ppolicy.ldif
collective.schema  core.ldif     cosine.schema  dyngroup.ldif    inetorgperson.schema  misc.ldif    nis.schema
pmi.ldif         ppolicy.schema
corba.ldif         core.schema   duaconf.ldif   dyngroup.schema  java.ldif             misc.schema  openldap.ldif
pmi.schema
```

Le schema de base est **core.schema**. D'autres schémas utiles sont notamment :

- inetorgperson.schema
- cosine.schema

Le chargement de ces deux fichiers de schémas nous permet de créer un objet pour une adresse email.

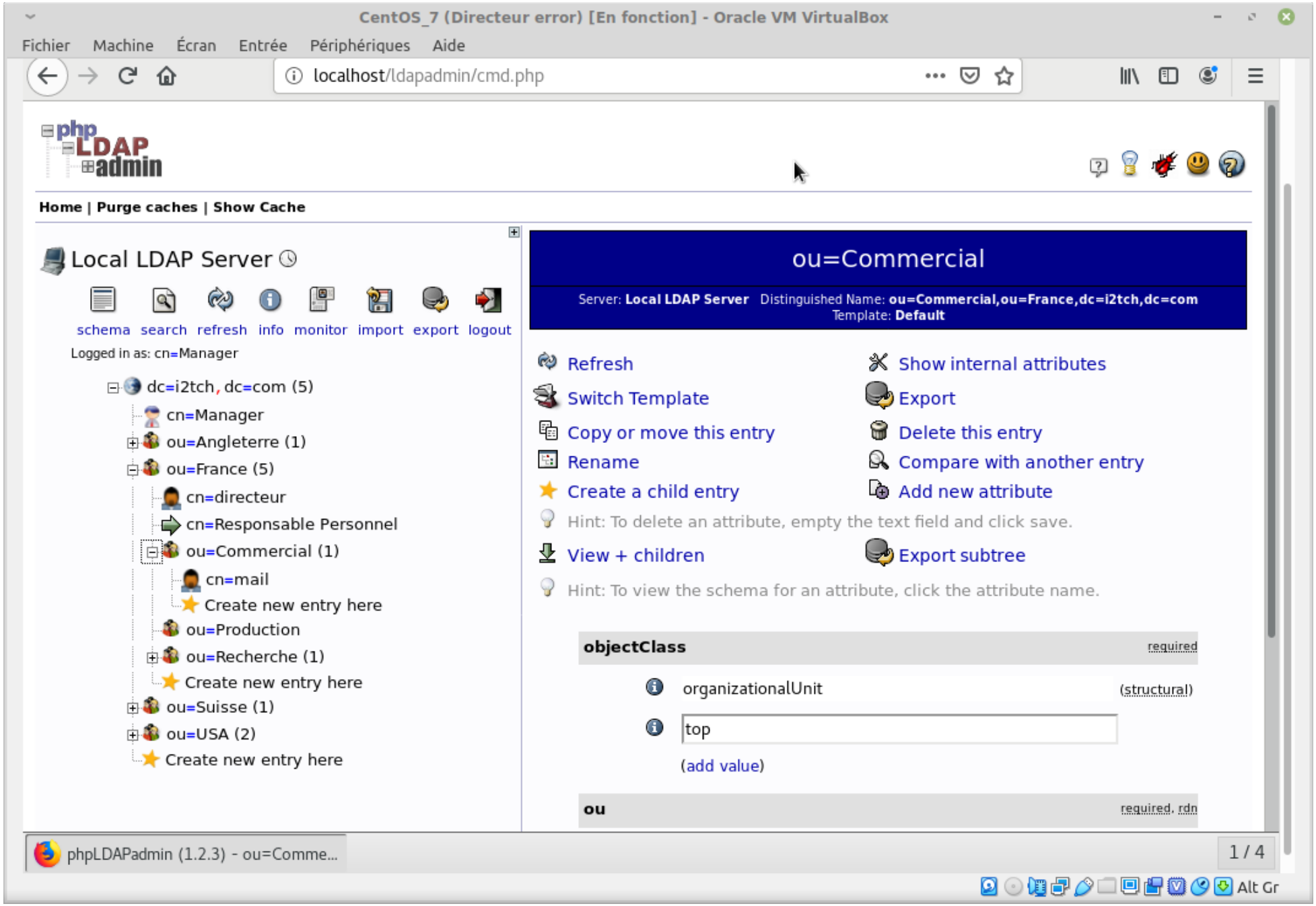
Créez le fichier LDIF **mail.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi mail.ldif
[root@centos7 ~]# cat mail.ldif
version: 1
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
```

Créez donc l'entrée **mail** en utilisant le fichier **mail.ldif** :

```
[root@centos7 ~]# ldapadd -f mail.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com"
```

Constatez maintenant le résultat avec phpLDAPadmin en cliquant sur l'icone **refresh** dans le panneau de gauche :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
localhost/ldapadmin/cmd.php
php LDAP admin
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial (1)
cn=mail
Create new entry here
ou=Production
ou=Recherche (1)
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
ou=Commercial
Server: Local LDAP Server Distinguished Name: ou=Commercial,ou=France,dc=i2tch,dc=com
Template: Default
Refresh
Show internal attributes
Switch Template
Export
Copy or move this entry
Delete this entry
Rename
Compare with another entry
Create a child entry
Add new attribute
Hint: To delete an attribute, empty the text field and click save.
View + children
Export subtree
Hint: To view the schema for an attribute, click the attribute name.
objectClass
required
organizationalUnit
(structural)
top
(add value)
ou
required, rdn
phpLDAPadmin (1.2.3) - ou=Comme...
1 / 4
Alt Gr

Les referrals

Il existe une autre entrée spéciale qui s'appelle un **referral**. Un referral est un pointeur vers une entrée vers un autre serveur LDAP. Pour illustrer ce point, créez le fichier LDIF **referral.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi referal.ldif
[root@centos7 ~]# cat referal.ldif
version: 1
dn: ou=Informatique,dc=i2tch,dc=com
objectClass: referral
objectClass: extensibleObject
objectClass: top
ref: ldap://ldap.i2tch.net/ou=i2tch.com,dc=i2tch,dc=net
ou: Informatique
```

Utilisez la commande ldapadd pour ajouter l'entrée au DIT :

```
[root@centos7 ~]# ldapadd -f referal.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -w fenestros
adding new entry "ou=Informatique,dc=i2tch,dc=com"
```

Constatez maintenant le résultat avec phpLDAPadmin en cliquant sur l'icone **refresh** dans le panneau de gauche :

LAB #2 - La Commande ldapsearch

Chaque annuaire contient une entrée **RootDSE**. Cette entrée est particulière puisque son DN est vide. Son rôle est de contenir les attributs opérationnels du serveur qui comportent des **extensions de contrôle** et **opérations** disponibles sur le serveur. Cette information est utilisée par le client LDAP lors de sa connexion afin de connaître ce que peut et ce que ne peut pas faire le serveur.

Afin de connaître le contenu du **RootDSE**, il convient d'utiliser la commande **ldapsearch**. Cette commande prend les options suivantes :

```
[root@centos7 ~]# ldapsearch  --help
ldapsearch: invalid option -- '-'
ldapsearch: unrecognized option --
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter    RFC 4515 compliant LDAP search filter
  attributes    whitespace-separated list of attribute descriptions
    which may include:
      1.1   no attributes
      *     all user attributes
      +     all operational attributes
Search options:
  -a deref   one of never (default), always, search, or find
  -A         retrieve attribute names only (no values)
  -b basedn  base dn for search
  -c         continuous operation mode (do not stop on errors)
  -E [!]<ext>[=<extparam>] search extensions (! indicates criticality)
             [!]domainScope              (domain scope)
             !dontUseCopy                (Don't Use Copy)
             [!]mv=<filter>              (RFC 3876 matched values filter)
             [!]pr=<size>[/prompt|noprompt] (RFC 2696 paged results/prompt)
             [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...]
                                         (RFC 2891 server side sorting)
             [!]subentries[=true|false]  (RFC 3672 subentries)
             [!]sync=ro[/<cookie>]       (RFC 4533 LDAP Sync refreshOnly)
                     rp[/<cookie>][/<slimit>] (refreshAndPersist)
             [!]vlv=<before>/<after>(/<offset>/<count>|:<value>)
                                         (ldapv3-vlv-09 virtual list views)
             [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]
             [!]<oid>[=:<b64value>] (generic control; no response handling)
  -f file    read operations from `file'
  -F prefix  URL prefix for files (default: file:///tmp/)
  -l limit   time limit (in seconds, or "none" or "max") for search
  -L         print responses in LDIFv1 format
```

```
  -LL        print responses in LDIF format without comments
  -LLL       print responses in LDIF format without comments
             and version
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -s scope   one of base, one, sub or children (search scope)
  -S attr    sort the results by attribute `attr'
  -t         write binary values to files in temporary directory
  -tt        write all values to files in temporary directory
  -T path    write files to directory specified by path (default: /tmp)
  -u         include User Friendly entry names in the output
  -z limit   size limit (in entries, or "none" or "max") for search
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
             ppolicy
             [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
             [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
             [!]relax
             [!]sessiontracking
             abandon, cancel, ignore (SIGINT sends abandon/cancel,
             or ignores response; if critical, doesn't wait for SIGINT.
             not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
  -I         use SASL Interactive mode
```

```
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
  -O props   SASL security properties
  -o <opt>[=<optparam>] general options
             nettimeout=<timeout> (in seconds, or "none" or "max")
             ldif-wrap=<width> (in columns, or "no" for no wrapping)
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

La syntaxe de la recherche du **RootDSE** est :

```
ldapsearch -x -s base -b "" "(objectclass=*)" +
```

Dans cette commande on peut constater des options :

Option	**Description**
-s base	Définit la portée de la recherche
-b “”	Définit un dn vide pour la recherche
“(objectclass=*)”	Définit ce que l'on recherche
+	Définit tous les attributs opérationnels

Le résultat obtenu est :

```
[root@centos7 ~]# ldapsearch -x -s base -b "" "(objectclass=*)" +
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: +
#

#
dn:
structuralObjectClass: OpenLDAProotDSE
configContext: cn=config
monitorContext: cn=Monitor
namingContexts: dc=i2tch,dc=com
supportedControl: 2.16.840.1.113730.3.4.18
supportedControl: 2.16.840.1.113730.3.4.2
supportedControl: 1.3.6.1.4.1.4203.1.10.1
supportedControl: 1.3.6.1.1.22
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.826.0.1.3344810.2.3
supportedControl: 1.3.6.1.1.13.2
supportedControl: 1.3.6.1.1.13.1
supportedControl: 1.3.6.1.1.12
supportedExtension: 1.3.6.1.4.1.1466.20037
supportedExtension: 1.3.6.1.4.1.4203.1.11.1
supportedExtension: 1.3.6.1.4.1.4203.1.11.3
supportedExtension: 1.3.6.1.1.8
supportedFeatures: 1.3.6.1.1.14
supportedFeatures: 1.3.6.1.4.1.4203.1.5.1
supportedFeatures: 1.3.6.1.4.1.4203.1.5.2
supportedFeatures: 1.3.6.1.4.1.4203.1.5.3
supportedFeatures: 1.3.6.1.4.1.4203.1.5.4
supportedFeatures: 1.3.6.1.4.1.4203.1.5.5
```

```
supportedLDAPVersion: 3
supportedSASLMechanisms: SCRAM-SHA-1
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: DIGEST-MD5
supportedSASLMechanisms: CRAM-MD5
ref: ldap://root.openldap.org
entryDN:
subschemaSubentry: cn=Subschema

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

A Faire - Utilisez le site web http://www.oid-info.com pour rechercher les **supportedFeatures**.

La commande ldapsearch utilisée ci-dessus a précisé une **portée** de base grâce à l'option **-s base**.

L'intérrogation de l'annuaire se fait avec une reqûete composée de 4 éléments :

Elément	**Description**
Base	Le point de départ de la reqûete
Attributs	La liste des attributs à retourner. Si vide ou *, tous les attributs sont retournés
Portée	Indique la portée de la reqûete. Elle peut être **Base**, **One** ou **Sub**
Filtre	Spécifie des critères a appliquer au attributs

La notion de la portée est la suivante :

- Base
  - Seul l'objet de base est fourni,
- One
  - Seuls les objets au premier niveau en dessous de l'objet de base sont fournis,
- Sub
  - Tous les objets en dessous de l'objet de base sont fournis.

La forme d'un filtre est :

- attribut, opérateur, valeur

L'opérateur est un des éléments suivants :

Opérateur	**Description**
=	égalité stricte
~=	égalité approximative
<=	inférieur ou égal
>=	supérieur ou égal
&	et logique
|	ou logique
!	non logique

La valeur peut être :

- une valeur exacte,
- une expression contenant le joker *.

Quand on veut trouver un caractère spécial, il convient de le remplacer avec une séquence spécifique :

Caractère	**Séquence**
*	\2A
(	\28
)	\29
\	\5C

Caractère	Séquence
Nul	\00

L'utilisation de ldapsearch peut être illustrée avec quelques exemples.

Dans l'exemple suivant, nous cherchons les entrées du type **ou** à partir de **ou=France,dc=i2tch,dc=com** :

```
[root@centos7 ~]# ldapsearch -x -b "ou=France,dc=i2tch,dc=com" "(objectClass=organizationalUnit)"
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=i2tch,dc=com> with scope subtree
# filter: (objectClass=organizationalUnit)
# requesting: ALL
#

# France, i2tch.com
dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

# Commercial, France, i2tch.com
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

# Recherche, France, i2tch.com
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

```
# Production, France, i2tch.com
dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires :

```
[root@centos7 ~]# ldapsearch -x -LLL -s children -b "ou=France,dc=i2tch,dc=com"
"(objectClass=organizationalUnit)"
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production
```

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires et avec un tri sur la valeur de l'ou :

```
[root@centos7 ~]# ldapsearch -x -LLL -S ou -s children -b "ou=France,dc=i2tch,dc=com"
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: dupont
sn: dupont

dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
```

```
dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Dans l'exemple suivant, nous cherchons les entrées **enfants** du type **ou** à partir de **ou=France,dc=i2tch,dc=com** sans commentaires, avec un tri sur la valeur de l'ou et en demandant une affichage plus lisible :

```
[root@centos7 ~]# ldapsearch -x -LLL -S ou -s children -u -b "ou=France,dc=i2tch,dc=com"
dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
ufn: Responsable Personnel, France, i2tch.com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
ufn: directeur, France, i2tch.com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com
ufn: dupont, Recherche, France, i2tch.com
objectClass: person
```

```
objectClass: top
cn: dupont
sn: dupont

dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
ufn: mail, Commercial, France, i2tch.com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
ufn: Commercial, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Production,ou=France,dc=i2tch,dc=com
ufn: Production, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
ufn: Recherche, France, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
```

Dans l'exemple suivant, nous cherchons les entrées du type **ou** et **cn** à partir de **ou=France,dc=i2tch,dc=com** en utilisant un fichier de filtre. Le fichier de filtre est **filtre** et contient **trois** lignes :

```
[root@centos7 ~]# vi filtre
[root@centos7 ~]# cat filtre
organizationalUnit
inetOrgPerson
```

Important - Ce fichier filtre DOIT comporter une ligne vide à la fin.

La commande est :

```
[root@centos7 ~]# ldapsearch -x -b "ou=France,dc=i2tch,dc=com" -f filtre "(objectClass=%s)" ou cn
# extended LDIF
#
# LDAPv3
# base <ou=France,dc=i2tch,dc=com> with scope subtree
# filter pattern: (objectClass=%s)
# requesting: ou cn
#

#
# filter: (objectClass=organizationalUnit)
#
# France, i2tch.com
dn: ou=France,dc=i2tch,dc=com
ou: France

# Commercial, France, i2tch.com
dn: ou=Commercial,ou=France,dc=i2tch,dc=com
ou: Commercial

# Recherche, France, i2tch.com
dn: ou=Recherche,ou=France,dc=i2tch,dc=com
```

```
ou: Recherche

# Production, France, i2tch.com
dn: ou=Production,ou=France,dc=i2tch,dc=com
ou: Production

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4

#
# filter: (objectClass=inetOrgPerson)
#
# mail, Commercial, France, i2tch.com
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
cn: mail

# search result
search: 3
result: 0 Success

# numResponses: 2
# numEntries: 1

#
# filter: (objectClass=)
#
# search result
search: 4
result: 0 Success
```

```
# numResponses: 1
```

LAB #3 - La Commande ldapmodify

La commande ldapmodify prend les options suivantes :

```
[root@centos7 ~]# ldapmodify --help
ldapmodify: invalid option -- '-'
ldapmodify: unrecognized option --
Add or modify entries from an LDAP server

usage: ldapmodify [options]
    The list of desired operations are read from stdin or from the file
    specified by "-f file".
Add or modify options:
  -a         add values (default is to replace)
  -c         continuous operation mode (do not stop on errors)
  -E [!]ext=extparam    modify extensions (! indicate s criticality)
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -S file    write skipped modifications to `file'
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                     one of "chainingPreferred", "chainingRequired",
                     "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
```

```
            [!]noop
            ppolicy
            [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
            [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
            [!]relax
            [!]sessiontracking
            abandon, cancel, ignore (SIGINT sends abandon/cancel,
            or ignores response; if critical, doesn't wait for SIGINT.
            not really controls)
  -h host   LDAP server
  -H URI    LDAP Uniform Resource Identifier(s)
  -I        use SASL Interactive mode
  -n        show what would be done but don't actually do it
  -N        do not use reverse DNS to canonicalize SASL host name
  -O props  SASL security properties
  -o <opt>[=<optparam>] general options
            nettimeout=<timeout> (in seconds, or "none" or "max")
            ldif-wrap=<width> (in columns, or "no" for no wrapping)
  -p port   port on LDAP server
  -Q        use SASL Quiet mode
  -R realm  SASL realm
  -U authcid SASL authentication identity
  -v        run in verbose mode (diagnostics to standard output)
  -V        print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W        prompt for bind password
  -x        Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file   Read password from file
  -Y mech   SASL mechanism
  -Z        Start TLS request (-ZZ to require successful response)
```

Afin d'illustrer l'utilisation de la commande **ldapmodify**, créez une fichier **prepa_modify.ldif** et éditez-le ainsi :

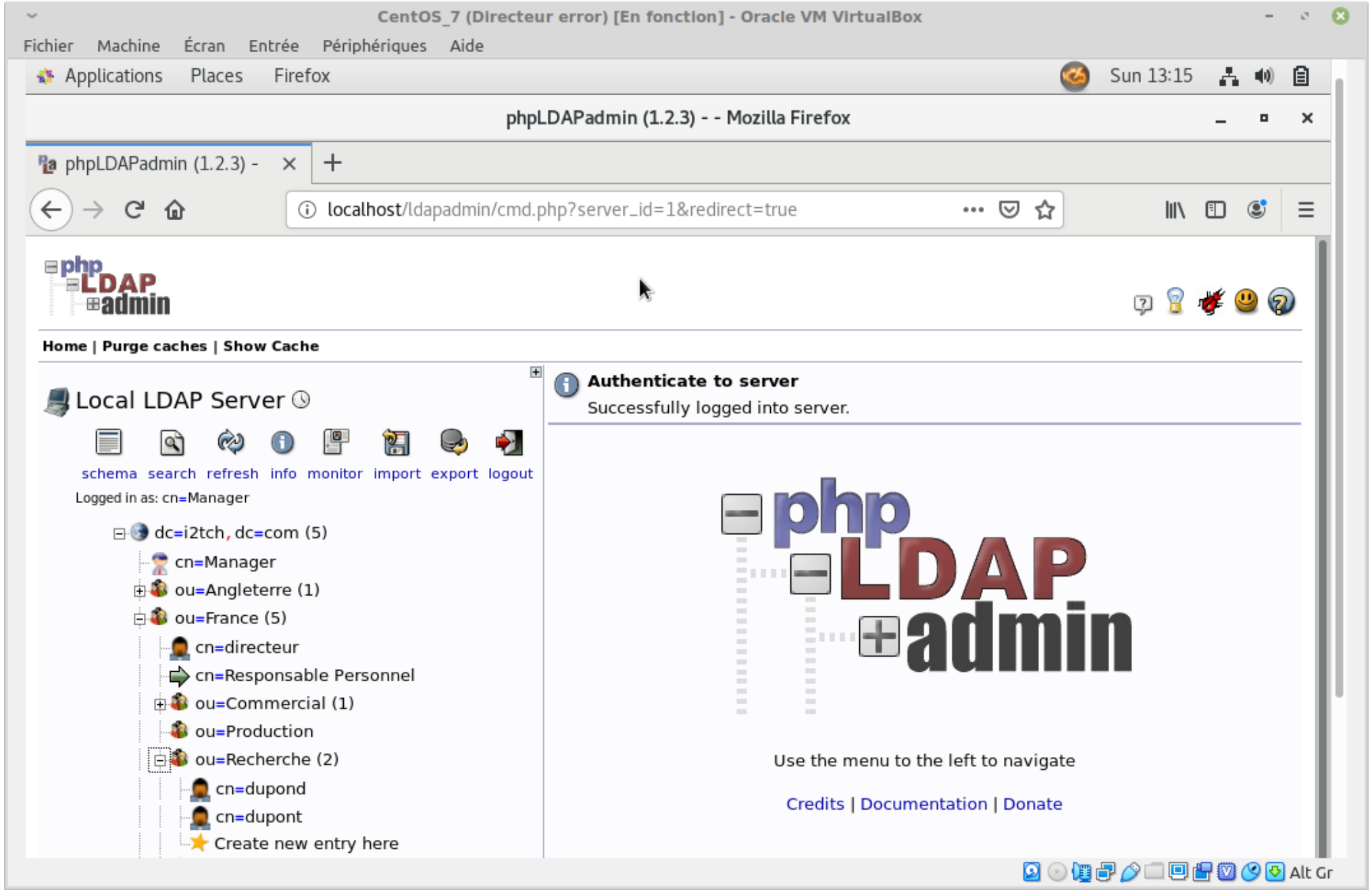
```
[root@centos7 ~]# vi prepa_modify.ldif
[root@centos7 ~]# cat prepa_modify.ldif
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
```

Saisissez ensuite la commande suivante :

```
[root@centos7 ~]# ldapadd -f prepa_modify.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -W
Enter LDAP Password: fenestros
adding new entry "cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

Important - Notez l'utilisation de l'option **-W** qui permet de demander au serveur un prompt pour le mot de passe au lieu de l'écrire en clair dans la commande elle-même. Notez donc que le mot de passe saisi ne sera **pas** en clair.

Visualisez votre DIT avec phpLDAPadmin. Vous constaterez un résultat similaire à celui-ci :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Sun 13:15
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/cmd.php?server_id=1&redirect=true
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial (1)
ou=Production
ou=Recherche (2)
cn=dupond
cn=dupont
Create new entry here
Authenticate to server
Successfully logged into server.
Use the menu to the left to navigate
Credits | Documentation | Donate
Alt Gr

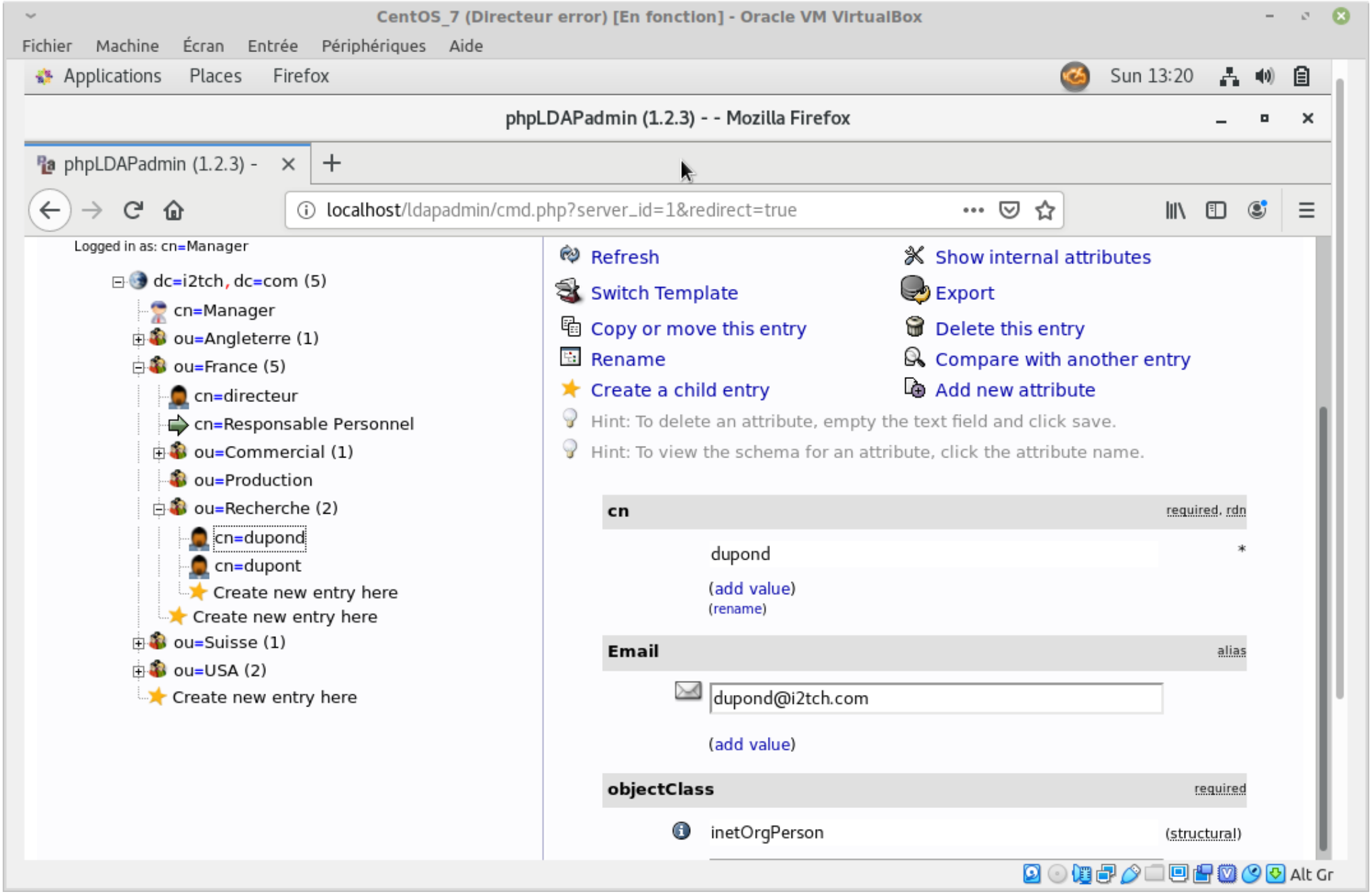
Nous allons maintenant utiliser la commande ldapmodify pour ajouter une adresse email à l'entrée **dupond**. Créez donc le fichier **modify.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi modify.ldif
[root@centos7 ~]# cat modify.ldif
dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
changetype: modify
add: mail
mail: dupond@i2tch.com
```

Saisissez maintenant la commande suivante :

```
[root@centos7 ~]# ldapmodify -f modify.ldif -x -D "cn=Manager,dc=i2tch,dc=com" -W
Enter LDAP Password: fenestros
modifying entry "cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com"
```

Visualisez votre DIT avec phpLDAPadmin. Vous constaterez un résultat similaire à celui-ci :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Sun 13:20
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/cmd.php?server_id=1&redirect=true
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial (1)
ou=Production
ou=Recherche (2)
cn=dupond
cn=dupont
Create new entry here
Create new entry here
ou=Suisse (1)
ou=USA (2)
Create new entry here
Refresh
Show internal attributes
Switch Template
Export
Copy or move this entry
Delete this entry
Rename
Compare with another entry
Create a child entry
Add new attribute
Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.
cn
required, rdn
dupond
*
(add value)
(rename)
Email
alias
dupond@i2tch.com
(add value)
objectClass
required
inetOrgPerson
(structural)
Alt Gr

LAB #4 - La Commande ldapdelete

Comme vous pouvez constater, vous avez deux entrées dans **ou=Recherche,ou=France,dc=i2tch,dc=com** :

- dupond
- dupont

Nous souhaitons maintenant supprimer l'entrée **dupont** en utilisant la commande **ldapdelete**. Les options de ldapdelete sont :

```
[root@centos7 ~]# ldapdelete --help
ldapdelete: invalid option -- '-'
ldapdelete: unrecognized option --
Delete entries from an LDAP server

usage: ldapdelete [options] [dn]...
    dn: list of DNs to delete. If not given, it will be readed from stdin
        or from the file specified with "-f file".
Delete Options:
  -c         continuous operation mode (do not stop on errors)
  -f file    read operations from `file'
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -r         delete recursively
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filter>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
```

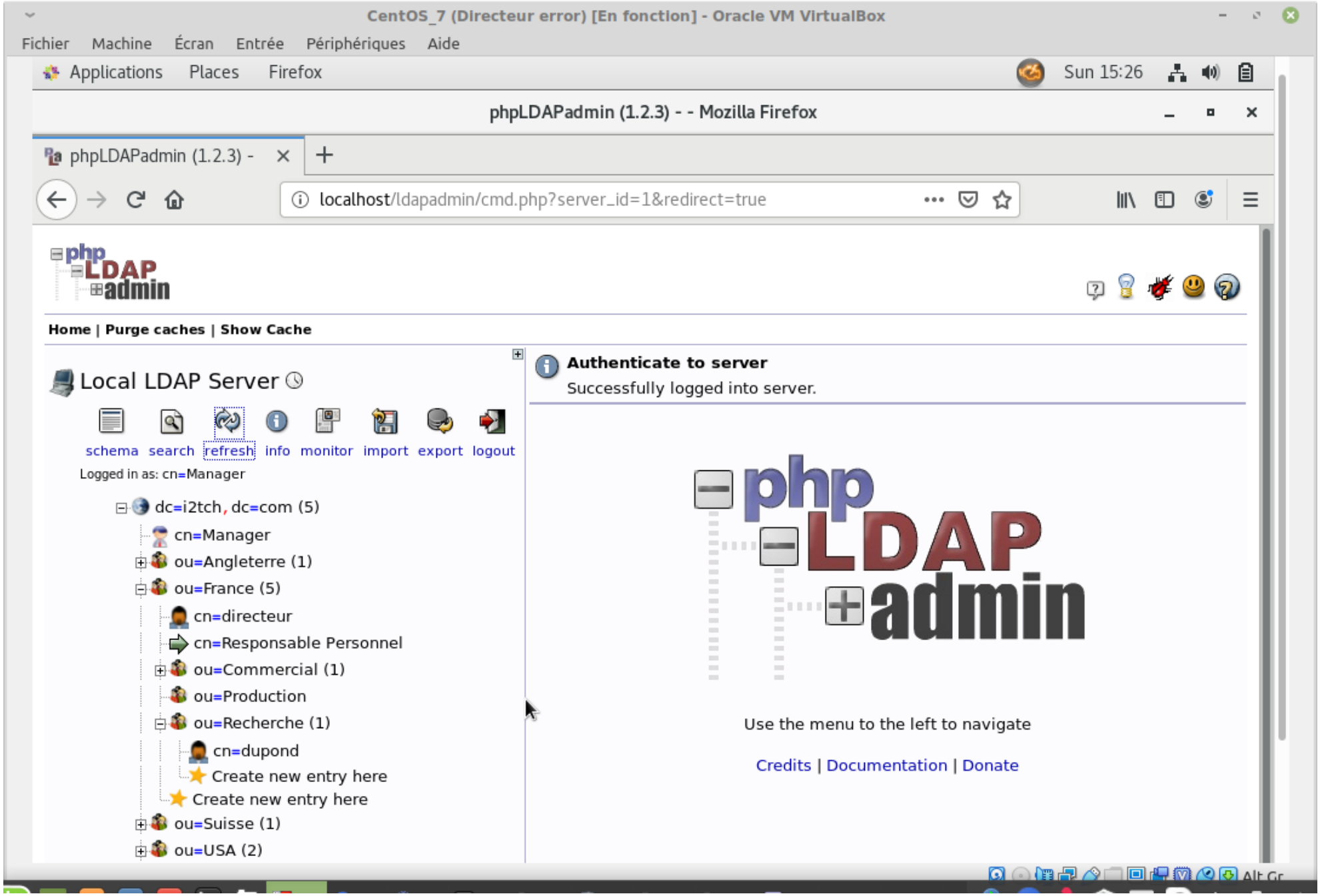
```
            [!]noop
            ppolicy
            [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
            [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
            [!]relax
            [!]sessiontracking
            abandon, cancel, ignore (SIGINT sends abandon/cancel,
            or ignores response; if critical, doesn't wait for SIGINT.
            not really controls)
  -h host   LDAP server
  -H URI    LDAP Uniform Resource Identifier(s)
  -I        use SASL Interactive mode
  -n        show what would be done but don't actually do it
  -N        do not use reverse DNS to canonicalize SASL host name
  -O props  SASL security properties
  -o <opt>[=<optparam>] general options
            nettimeout=<timeout> (in seconds, or "none" or "max")
            ldif-wrap=<width> (in columns, or "no" for no wrapping)
  -p port   port on LDAP server
  -Q        use SASL Quiet mode
  -R realm  SASL realm
  -U authcid SASL authentication identity
  -v        run in verbose mode (diagnostics to standard output)
  -V        print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W        prompt for bind password
  -x        Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file   Read password from file
  -Y mech   SASL mechanism
  -Z        Start TLS request (-ZZ to require successful response)
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# ldapdelete -x -D "cn=Manager,dc=i2tch,dc=com" -W
"cn=dupont,ou=Recherche,ou=France,dc=i2tch,dc=com"
Enter LDAP Password: fenestros
```

Important - Notez l'absence d'une confirmation de la suppression.

Rafraichissez phpLDAPadmin. Vous constaterez un résultat similaire à celui-ci :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Sun 15:26
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/cmd.php?server_id=1&redirect=true
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial (1)
ou=Production
ou=Recherche (1)
cn=dupond
Create new entry here
Create new entry here
ou=Suisse (1)
ou=USA (2)
Authenticate to server
Successfully logged into server.
Use the menu to the left to navigate
Credits | Documentation | Donate

Supprimer maintenant le referral mis en place tout à l'heure :

```
[root@centos7 ~]# ldapdelete -x -M -D "cn=Manager,dc=i2tch,dc=com" -W "ou=Informatique,dc=i2tch,dc=com"
Enter LDAP Password: fenestros
```

LAB #5 - La Commande slapadd

Jusqu'à maintenant nous avons apporter des modifications à la base LDAP **en ligne**, autrement dit pendant que le serveur était en cours de fonctionnement. Il est aussi possible d'apporter des modifications quand le serveur est arrêté.

Pour faire ceci, on dispose de la commande **slapadd**. Les options de la commande slapadd sont :

```
[root@centos7 ~]# slapadd --help
slapadd: invalid option -- '-'
usage: slapadd [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
    [-g] [-n databasenumber | -b suffix]
    [-l ldiffile] [-j linenumber] [-q] [-u] [-s] [-w]
```

Créez d'abord le fichier LDIF **slapadd.ldif** et éditez-le ainsi :

```
[root@centos7 ~]# vi slapadd.ldif
[root@centos7 ~]# cat slapadd.ldif
dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

Arrêtez maintenant le service slapd :

```
[root@centos7 ~]# systemctl stop slapd
[root@centos7 ~]# systemctl status slapd
```

```
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Sun 2020-01-12 15:31:13 CET; 5s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
  Process: 1061 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited, status=0/SUCCESS)
  Process: 923 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 1077 (code=exited, status=0/SUCCESS)

Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=0 BIND dn="cn...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=0 RESULT tag=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=1 DEL dn="ou=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=1 RESULT tag=...
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 op=2 UNBIND
Jan 12 15:27:38 centos7.fenestros.loc slapd[1077]: conn=1008 fd=11 closed
Jan 12 15:31:13 centos7.fenestros.loc slapd[1077]: daemon: shutdown requested...
Jan 12 15:31:13 centos7.fenestros.loc systemd[1]: Stopping OpenLDAP Server Da...
Jan 12 15:31:13 centos7.fenestros.loc slapd[1077]: slapd shutdown: waiting fo...
Jan 12 15:31:13 centos7.fenestros.loc systemd[1]: Stopped OpenLDAP Server Dae...
Hint: Some lines were ellipsized, use -l to show in full.
```

Saisissez maintenant la commande suivante :

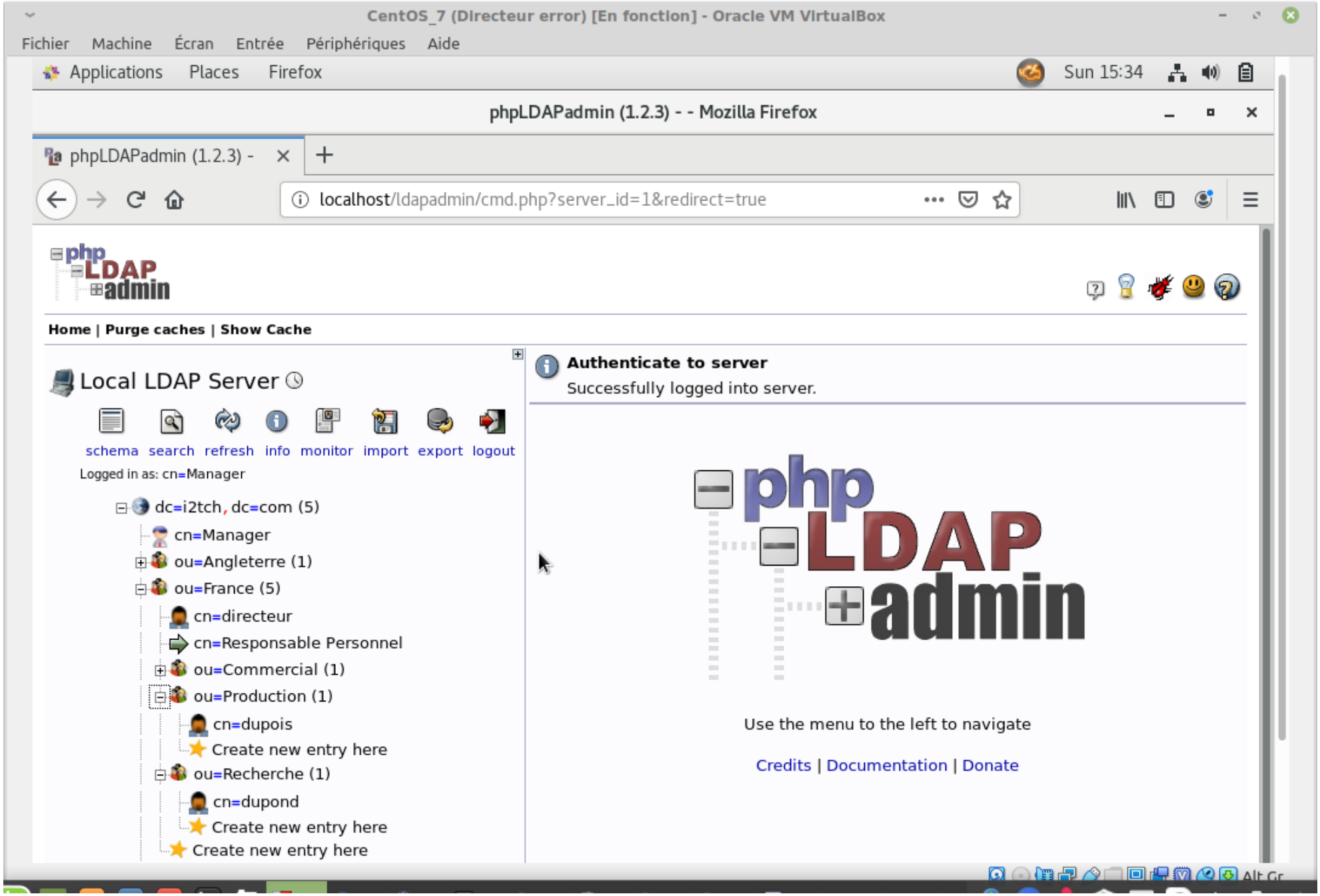
```
[root@centos7 ~]# slapadd -b "dc=i2tch,dc=com" -l slapadd.ldif
_################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Démarrez le service slapd :

```
[root@centos7 ~]# systemctl start slapd
[root@centos7 ~]# systemctl status slapd
```

```
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-01-12 15:33:21 CET; 3s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
  Process: 6693 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited, status=0/SUCCESS)
  Process: 6651 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 6695 (slapd)
   CGroup: /system.slice/slapd.service
           └─6695 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Jan 12 15:33:21 centos7.fenestros.loc runuser[6679]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6681]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6683]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6685]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6687]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6689]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc runuser[6691]: pam_unix(runuser:session...
Jan 12 15:33:21 centos7.fenestros.loc slapd[6693]: @(#) $OpenLDAP: slapd 2.4....
                                                          mockbuild@x86-01.b...
Jan 12 15:33:21 centos7.fenestros.loc slapd[6695]: slapd starting
Jan 12 15:33:21 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Dae...
Hint: Some lines were ellipsized, use -l to show in full.
```

Rafraichissez phpLDAPadmin. Vous constaterez un résultat similaire à celui-ci :


CentOS_7 (Directeur error) [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places Firefox
Sun 15:34
phpLDAPadmin (1.2.3) - - Mozilla Firefox
phpLDAPadmin (1.2.3) -
localhost/ldapadmin/cmd.php?server_id=1&redirect=true
Home | Purge caches | Show Cache
Local LDAP Server
schema search refresh info monitor import export logout
Logged in as: cn=Manager
dc=i2tch, dc=com (5)
cn=Manager
ou=Angleterre (1)
ou=France (5)
cn=directeur
cn=Responsable Personnel
ou=Commercial (1)
ou=Production (1)
cn=dupois
Create new entry here
ou=Recherche (1)
cn=dupond
Create new entry here
Create new entry here
Authenticate to server
Successfully logged into server.
Use the menu to the left to navigate
Credits | Documentation | Donate
Alt Gr

LAB #6 - Maintenance d'une base de données LDAP

6.1 - La commande slapcat

La commande **slapcat** produit un fichier LDIF à partir d'une base de données slapd.

L'exportation ne produit **pas** un fichier hiérarchique. Pour cette raison, le fichier peut être utilisé par la commande **slapadd** mais ne peut **pas** être utilisé par la commande **ldapadd**.

Les options de cette commande sont :

```
[root@centos7 ~]# slapcat --help
slapcat: invalid option -- '-'
usage: slapcat [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
    [-g] [-n databasenumber | -b suffix] [-l ldiffile] [-a filter] [-s subtree] [-H url]
```

Saisissez donc les commandes suivantes :

```
[root@centos7 ~]# systemctl stop slapd
[root@centos7 ~]# slapcat -b "dc=i2tch,dc=com" -l backup.ldif
```

Consultez maintenant le contenu du fichier **backup.ldif** :

```
[root@centos7 ~]# cat backup.ldif
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple
structuralObjectClass: organization
entryUUID: 7f60340c-c739-1039-9642-efd3014890db
```

```
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143851Z
entryCSN: 20200109143851.158182Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143851Z

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
structuralObjectClass: organizationalRole
entryUUID: 7f611b60-c739-1039-9643-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143851Z
entryCSN: 20200109143851.164106Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143851Z

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France
structuralObjectClass: organizationalUnit
entryUUID: a622df86-c739-1039-9644-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.187387Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
```

```
structuralObjectClass: organizationalUnit
entryUUID: a624e218-c739-1039-9645-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.200565Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: a6253092-c739-1039-9646-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.202576Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production
structuralObjectClass: organizationalUnit
entryUUID: a625d74a-c739-1039-9647-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.206843Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
```

```
objectClass: top
ou: Suisse
structuralObjectClass: organizationalUnit
entryUUID: a6261b24-c739-1039-9648-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.208581Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: a62660e8-c739-1039-9649-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.210367Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA
structuralObjectClass: organizationalUnit
entryUUID: a626bca0-c739-1039-964a-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.212715Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z
```

```
dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial
structuralObjectClass: organizationalUnit
entryUUID: a626fc4c-c739-1039-964b-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.214345Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche
structuralObjectClass: organizationalUnit
entryUUID: a6274a12-c739-1039-964c-efd3014890db
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200109143956Z
entryCSN: 20200109143956.216336Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200109143956Z

dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject
structuralObjectClass: alias
entryUUID: bbb6f964-c7d3-1039-905e-0bb7ee6decc3
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110090254Z
```

```
entryCSN: 20200110090254.886500Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110090254Z

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321
structuralObjectClass: person
entryUUID: c0bba43a-c7da-1039-9f6f-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110095309Z
entryCSN: 20200110095309.782800Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110095309Z

dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre
structuralObjectClass: organizationalUnit
entryUUID: 95e2dba6-c7e0-1039-9f70-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.878156Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
```

```
ou: Sales
structuralObjectClass: organizationalUnit
entryUUID: 95e965d4-c7e0-1039-9f71-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.921008Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith
structuralObjectClass: person
entryUUID: 95f02de2-c7e0-1039-9f72-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103454Z
entryCSN: 20200110103454.965453Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110103454Z

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=co
 m
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
structuralObjectClass: person
entryUUID: 95f62710-c7e0-1039-9f73-31eb8911c0ef
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110103455Z
entryCSN: 20200110103455.004608Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
```

```
modifyTimestamp: 20200110103455Z

dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info
structuralObjectClass: inetOrgPerson
entryUUID: aa1bfcb0-c808-1039-900b-092b75c3c5a4
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200110152148Z
entryCSN: 20200110152148.676173Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200110152148Z

dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
structuralObjectClass: inetOrgPerson
entryUUID: 96de82d0-c97f-1039-92ab-977e121b768c
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200112120537Z
mail: dupond@i2tch.com
entryCSN: 20200112121812.106114Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200112121812Z

dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
```

```
cn: dupois
sn: dupois
structuralObjectClass: inetOrgPerson
entryUUID: 066ceaf6-c994-1039-8f6f-ab1664534830
creatorsName: cn=Manager,dc=i2tch,dc=com
createTimestamp: 20200112143154Z
entryCSN: 20200112143154.765140Z#000000#000#000000
modifiersName: cn=Manager,dc=i2tch,dc=com
modifyTimestamp: 20200112143154Z
```

6.2 - La commande slapindex

La commande **slapindex** crée ou met à jour les index définis pour une base de données slapd.

Les options de cette commande sont :

```
[root@centos7 ~]# slapindex --help
slapindex: invalid option -- '-'
usage: slapindex [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-c]
    [-g] [-n databasenumber | -b suffix] [attr ...] [-q] [-t]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slapindex -b "dc=i2tch,dc=com" -v
indexing id=00000001
indexing id=00000002
indexing id=00000003
indexing id=00000004
indexing id=00000005
indexing id=00000006
indexing id=00000007
indexing id=00000008
indexing id=00000009
```

```
indexing id=0000000a
indexing id=0000000b
indexing id=0000000c
indexing id=0000000d
indexing id=0000000e
indexing id=0000000f
indexing id=00000010
indexing id=00000011
indexing id=00000013
indexing id=00000015
indexing id=00000016
```

6.3 - La commande slapdn

La commande **slapdn** vérifie la cohérence d'une entrée spécifiée par rapport au(x) schéma(s) défini(s) pour slapd.

Les options de cette commande sont :

```
[root@centos7 ~]# slapdn --help
slapdn: invalid option -- '-'
usage: slapdn [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]]
    [-N | -P] DN [...]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slapdn cn=smith,dc=i2tch,dc=com
DN: <cn=smith,dc=i2tch,dc=com> check succeeded
normalized: <cn=smith,dc=i2tch,dc=com>
pretty:     <cn=smith,dc=i2tch,dc=com>
```

6.4 - La commande slaptest

La commande **slaptest** vérifie la syntaxe des fichiers de configuration de slapd.

Les options de cette commande sont :

```
[root@centos7 ~]# slaptest --help
slaptest: invalid option -- '-'
usage: slaptest [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]] [-n databasenumber] [-
u] [-Q]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slaptest -u
config file testing succeeded
```

6.5 - La commande slapauth

La commande **slapauth** vérifie la correspondance entre les ID et les DN.

Les options de cette commande sont :

```
root@centos7 ~]# slapauth --help
slapauth: invalid option -- '-'
usage: slapauth [-v] [-d debuglevel] [-f configfile] [-F configdir] [-o <name>[=<value>]]
    [-U authcID] [-X authzID] [-R realm] [-M mech] ID [...]
```

Saisissez donc la commande suivante :

```
[root@centos7 ~]# slapauth -v U smith X u :smith
ID: <U> check succeeded
authcID:     <uid=u,cn=auth>
```

```
ID: <smith> check succeeded
authcID:     <uid=smith,cn=auth>
ID: <X> check succeeded
authcID:     <uid=x,cn=auth>
ID: <u> check succeeded
authcID:     <uid=u,cn=auth>
ID: <:smith> check succeeded
authcID:     <uid=:smith,cn=auth>
```

Démarrez slapd :

```
[root@centos7 ~]# systemctl start slapd
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-01-12 15:50:26 CET; 5s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
  Process: 11958 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited,
status=0/SUCCESS)
  Process: 11915 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 11966 (slapd)
   CGroup: /system.slice/slapd.service
           └─11966 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Jan 12 15:50:26 centos7.fenestros.loc runuser[11943]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc runuser[11945]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc runuser[11947]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc runuser[11949]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc runuser[11951]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc runuser[11953]: pam_unix(runuser:sessio...
```

```
Jan 12 15:50:26 centos7.fenestros.loc runuser[11955]: pam_unix(runuser:sessio...
Jan 12 15:50:26 centos7.fenestros.loc slapd[11958]: @(#) $OpenLDAP: slapd 2.4...
                                                              mockbuild@x86-01....
Jan 12 15:50:26 centos7.fenestros.loc slapd[11966]: slapd starting
Jan 12 15:50:26 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Dae...
Hint: Some lines were ellipsized, use -l to show in full.
```

<html>

Copyright © 2020 Hugh Norris.

</html>